

PRIMERGY BX900 Blade Server Systems

ServerView Management Blade
User Interface Description

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Copyright © 2014 Fujitsu Technology Solutions GmbH.

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trade names and/or trademarks of their respective manufacturers.

- The contents of this manual may be revised without prior notice.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.

Microsoft, Windows, Windows Server, and Hyper V are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

Before reading this manual

High safety use

This product has been designed and manufactured for general uses such as general office use, personal use, domestic use and normal industrial use. It has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk to life or body if such safety cannot be ensured.

These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

Technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan

Documents produced by FUJITSU may contain technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization in accordance with the above law.

Contents

1	Introduction	7
1.1	Notational Conventions	8
1.2	Target Group	8
2	PRIMERGY BX Blade Server System – Overview	9
2.1	The Blade Server Concept	9
2.2	Blade Server Management	9
2.2.1	Features of the ServerView Management Blade	9
2.2.2	Redundancy of the ServerView Management Blade	11
2.2.3	Console Redirection	11
3	Telnet Interface	13
3.1	Entering the console mode	13
3.2	Console main menu	14
3.3	Management Agent	15
3.3.1	Management Agent Information	16
3.3.2	Management Blade	18
3.3.3	System Information	19
3.3.4	Server Blade	20
3.3.5	Storage Server Blade	24
3.3.6	Connection Blade	25
3.3.7	User Management	26
3.3.8	Blue Screen	28
3.3.9	Event Log	29
3.3.10	Set System Default	30
3.3.11	Server Blade CMOS Backup/Restore	31
3.3.12	Connection Blade Configuration Backup/Restore	32
3.3.13	Power Consumption	33
3.3.14	LDAP Authentication	34
3.3.15	VLAN Information	35
3.3.16	I2C Bus Management	35
3.3.17	Management Blade Configuration Backup/Restore	35
3.3.18	Management Blade Base Configuration Backup/Restore	36
3.4	Emergency Management Port	36
3.5	Console Redirection	36
3.6	TFTP Update	37
3.7	Logout	38
3.8	Change Management Role To Slave	38
3.9	System Information Dump	39
3.10	Command Line Interface	40

3.11	Account Management	40
4	Web User Interface	41
4.1	Login	41
4.2	The Start Page	42
4.3	Changing the User Name and Password	48
4.4	MMB firmware upgrade via TFTP	50
4.5	MMB firmware update via USB	51
4.6	MMB firmware update via HTTP	52
5	Power Management	53
5.1	Power Consumption Display	54
5.2	Control via Tabs	54
5.2.1	History Tab	55
5.2.2	Power Switch Tab	56
5.2.3	Input Power Limit Tab	59
5.2.4	Consumption Tab	61
6	Global User Management	65
6.1	Configuring an Active Directory Server	65
6.1.1	Installing the Windows Active Directory Server	65
6.1.2	Creating the LDAP Structure (based on Microsoft Active Directory)	66
6.1.3	Assigning Domain Users to the MMB	67
6.1.4	Setting up the Management Blade	68
6.1.5	Logging in on the Management Blade as an AD User	69
6.2	Configuring an openLDAP Server	70
6.2.1	Base Configuration of openLDAP	70
6.2.2	Creating the LDAP Structure (Based on openLDAP)	71
6.2.3	Assigning Domain Users to the MMB	72
6.2.4	Setting up the Management Blade	72
6.2.5	Logging in on the Management Blade as an openLDAP User	75
6.3	Configuring an eDirectory Server	76
6.3.1	Installing the eDirectory Server	76
6.3.2	Creating the LDAP Structure (Based on eDirectory)	76
6.3.3	Assigning Domain Users to the MMB	77
6.3.4	Setting up the Management Blade	78
6.3.5	Logging in on the Management Blade as an eDirectory User	80
7	Web User Interface Icons Overview	81
	Abbreviations	83
	Related Publications	89

1 Introduction

The PRIMERGY BX Blade Server Systems accommodate two hot-swappable, redundant ServerView management blades (standard equipment is one): an integrated management solution for complete remote administration of the blade server system. For a complete feature list, see [section "Features of the ServerView Management Blade" on page 9](#).



Figure 1: ServerView management blade

Further information is available online from the Fujitsu manuals server:

- PRIMERGY BX900 Blade Server – Operating Manual
- PRIMERGY ServerView Suite – ServerView Deployment Manager
- PRIMERGY BX900 Blade Servers – Manuals for various connection blades
- ServerView Operations Manager User Guide

i For further information on updating BX components please refer to the Operating Manual of your BX system.

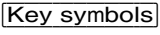
i Fujitsu manuals server at:

For the global market: <http://manuals.ts.fujitsu.com>

For the Japanese market: <http://jp.fujitsu.com/platform/server/primergy/manual>

1.1 Notational Conventions

The following notational conventions are used in this manual:

	Caution	This symbol points out hazards that can lead to personal injury, loss of data, or damage to equipment.
		This symbol highlights important information and tips.
		This symbol refers to a step that you must carry out in order to continue with the procedure.
<i>italic</i>		Commands, menu items, names of buttons, options, file names, and path names are written in <i>italic</i> letters in the text.
<variable>		Marked variables that must be replaced by current values.
fixed font		System output is written using a fixed font.
semi-bold fixed font		Commands to be entered through the keyboard are written in a semi-bold fixed font.
		Keys are presented according to their representation on the keyboard. If capital letters are to be entered explicitly, then the Shift key is shown, e.g.  -  for A. If two keys need to be pressed at the same time, then this is indicated by placing a hyphen between the two key symbols.

If there are references to text or sections of text in this manual, then the chapter or section heading is placed in the reference, and the page stated refers to the page on which the chapter or section begins.

1.2 Target Group

This manual is intended for system administrators, network administrators, and service technicians that have a basic knowledge of hardware and software. The manual informs the reader of the fundamentals of blade server monitoring and documents the requirements for the use of the ServerView management blade.

2 PRIMERGY BX Blade Server System – Overview

In this chapter an overview is given of the blade server system. The concept underlying this system is explained, and its major features are described. Furthermore, the system component is described that enables the user to communicate with the system.

2.1 The Blade Server Concept

A traditional server is a device that includes a multitude of components to do many different jobs at the same time. Servers like this are distinguished by the number of CPUs they use, the number of hard disks that can be plugged in, and the number of PCI cards that can be used to connect them to other devices such as external storage systems or networks.

Further development has made it necessary to treat the issues of CPU power and storage capacity separately. Rack optimized servers enable the system administrator to make adjustments in both fields according to the level that is needed.

At the next step, the blade server concept is reached, where I/O functions, too, are separated from the CPU. A blade server system typically consists of a number CPU boards, known as server blades, together with some connection blades, which are the I/O modules, and finally a redundantly configured pair of ServerView management blades, enabling the user to monitor and control the system on the whole.

All data traffic moving to and from the system is handled via TCP/IP over a LAN cable.

The outsourcing of the power supply unit and the use of low-voltage CPUs help to reduce the size of a server blade. Thus, a high density is achieved for the system with very little power consumption compared to traditional servers.

2.2 Blade Server Management

When performing administrative tasks for the blade server system, the user relies on functions provided by a system component called the ServerView management blade. There are two ServerView management blades in a blade server system, in order to ensure redundancy.

The user gets access to the functions provided by the ServerView management blade, either via a web user interface, or via a console menu using the Telnet protocol. Both ways of communication are described in more detail in the next two chapters of this manual (see [chapter "Telnet Interface"](#) and [chapter "Web User Interface"](#)).

2.2.1 Features of the ServerView Management Blade

Within the blade server system the ServerView management blade is equipped with a number of features, which are described in this section.

Controller

The ServerView management blade is equipped with an AMCC PPC405EP controller.

Supported programs

The ServerView management blade is compliant with IPMI (Internet Protocol Multicast Initiative) 2.0. It supports schemes like FRU (Field Replaceable Units), SEL (System Event Log), and SDR (Sensor Data Records). It also allows the configuration of a watchdog timer.

Communication with the server blades

The ServerView management blade communicates with the server blades via an I²C bus. An IPMB interface is provided to support the user, when performing hardware monitoring tasks for the server blades.

Communication with the connection blades

To enable communication with the connection blades, a CLI interface is provided. It allows to configure settings of the connection blades, such as the IP address, the IP mask, or the IP gateway address.

Hardware monitoring

The hardware monitoring functions provided by the ServerView management blade include:

- Monitoring temperature of each server blade via the IPMB interface
- Monitoring the status of the system fans
- Setting the system fans to an optimum speed
- Monitoring the status of the power supply modules
- Monitoring the temperature of the connection blades via the I²C bus

Event repository

To store messages on events that occur in the system environment, the ServerView management blade is equipped with an event repository, providing a 2 x 32 MB SDRAM.

Auto configuration

The management function auto configuration is used to back up system parameters to a ROM, which is located on the management blade. It also provides the possibility to restore these parameters if required. This reduces the risk if system configuration data have been corrupted or lost.

SSL (Secure Socket Layer)

The Manager Blade provides SSL for network data privacy for Telnet as well as for HTTP connections. Fujitsu Technology Solutions recommend to replace the default system certificate key to use the secured environment.

2.2.2 Redundancy of the ServerView Management Blade

Of the two ServerView management blades within the blade server system, one will take over the role of the master, who is in charge of the server management, while the other one will remain in a standby status as a redundant component. The two components have the same IP address, but their MAC addresses differ from each other.

The management blade in slot 1 becomes the master management blade by default.

The master blade and the redundant blade communicate symmetrically with each other via a TX/RX serial interface. As soon as the master fails to work properly, for instance, when unplugged by the system administrator, the standby component will take over control of the server management.

Fail-over scenario

When the redundant ServerView management blade takes over control from the master, it will behave according to the following scenario:

- Issue an ICMP broadcast ping to update the ARP table and connection the IP filtering table, in order to adjust them with regard to the new MAC address
- Define a proprietary protocol in L2, which is used for remote communication

If communication between master and redundant component via the serial interface has broken down, these components can continue to communicate by sending IP broadcast packages, using the MAC addresses.

2.2.3 Console Redirection

When using the console redirection feature, the management of the blade server system may be executed in remote control mode. To support this mode, the ServerView management blade acts as the console redirection agent.

3 Telnet Interface

Within the blade server system a console menu is provided for server management, using the Telnet protocol. A number of configuration activities can be performed via this menu, e.g. IP address configuration or hardware status monitoring. The menu is described in this chapter.

 New features and functions are no longer upgraded and maintained in the *Console menu* interface described starting with [3.2 on page 14](#), but only in the *Command Line Interface* (also known as "SM-CLP" or "SMASH CLP Shell", see [3.10 on page 40](#)) and via SNMP interface.

You find the documentation of the SMASH CLP Shell in the MMB Web User Interface help pages:

1. Click the *Help* field at the far right below the Fujitsu logo.
2. Click *On Contents*.
3. Navigate to section *Available Help Texts, Notes*.
4. In the *OEM SM CLP targets and concept* item, click *concept* to open an introduction and *targets* to see details.

3.1 Entering the console mode

To enter the console mode a connection from a PC to the serial port of the blade server system has to be established first. For this purpose a RS232 cable (null modem cable) is used. An RX/TX signal will then be exchanged via this cable.

After the connection has been established, the HyperTerminal option is called up on the PC.

The parameters for this option are to be set as follows:

Baud rate	115200
Parity bits	None
Data bits	8
Stop bits	1
Flow control	None
Terminal type	VT100

LAN interface connection

The console mode can also be entered via LAN. In this case, the Telnet client is called up, and the login procedure is performed using the management blade IP address.

The settings are then as follows:

Host IP address Service LAN	192.138.1.1 (default for a management blade address, the slave - when active - has the same address as the master)
Host IP address Management LAN	192.168.1.10 (default for a management blade address, the slave - when active - has the same address as the master)
Telnet port	Same as the Telnet port configured for the management blade (default port: 3172)
SSHv2 port	22

After these parameters have been set, the blade server system is started.

When using the serial port, firstly a number of messages concerning the system appears on the screen.

After approximately five seconds a welcome screen is displayed.

The user is requested to enter a user name and eventually a password, to be admitted to the console main menu.

The default user name and the default password are both 'admin'.

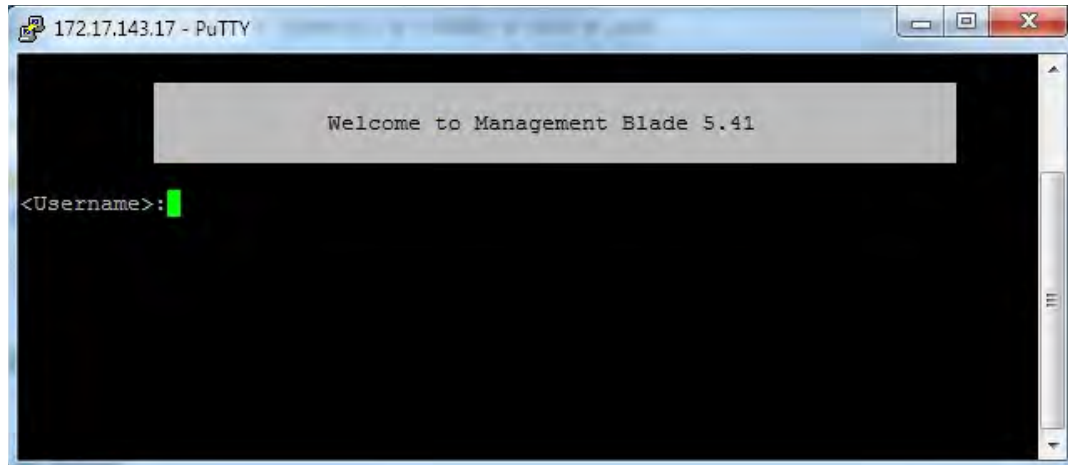


Figure 2: Welcome screen for access to the console menu

3.2 Console main menu

i New features and functions are no longer upgraded and maintained in the *Console menu* interface described starting here, but only in the *Command Line Interface* (also known as "SM-CLP" or "SMASH CLP Shell", see [3.10 on page 40](#)) and via SNMP interface.

The console main menu looks like this:

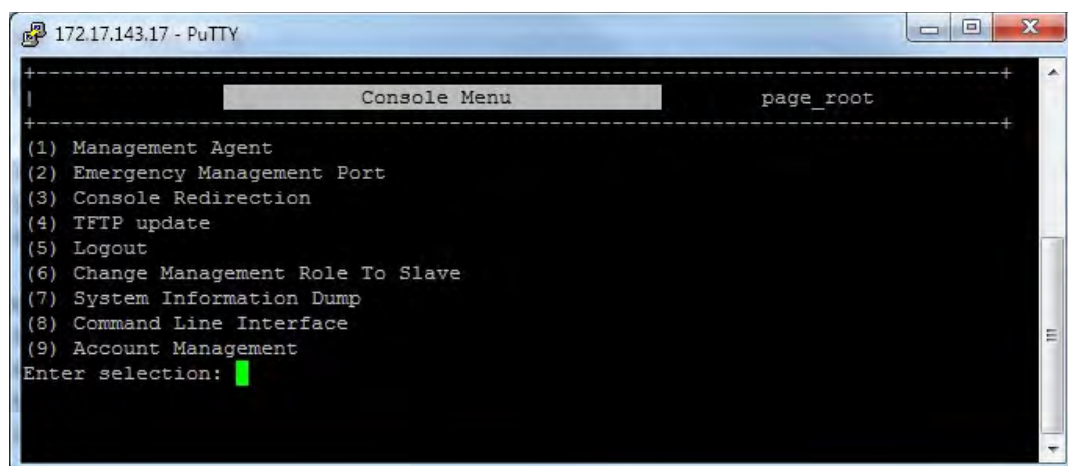


Figure 3: Console main menu

There are nine items in the console main menu:

1. Management Agent (see [3.3 on page 15](#))

This item provides several options for the management of the whole blade server system, including management blades and connection blades.

2. Emergency Management Port (see [3.4 on page 36](#))

This item provides an interface to send IPMI messages to a management blade in case of an emergency. It can also be used for debugging purposes.

3. Console Redirection (see [3.5 on page 36](#))

This item is used to configure the console redirection mode. The selected console redirection target will be active after the next boot.

4. TFTP Update (see [3.6 on page 37](#))

This item is used to update the management blade firmware.

5. Logout (see [3.7 on page 38](#))

This item is used to logout from the system.

6. Change Management Role To Slave (see [3.8 on page 38](#))

This item is used to change the management blade role to slave.



If only one management blade is available, the menu item header is dynamically changed to "Reboot Management Blade". In this state, every reboot is executed immediately.

7. System Information Dump (see [3.9 on page 39](#))

This item is used to display consecutive lists of information.

8. Command Line Interface (see [3.10 on page 40](#))

This item is used to get whole chassis information.

9. Account Management (see [3.11 on page 40](#))

This item is used to change the user password.

The items of the console main menu are described in more detail in the following sections.

3.3 Management Agent

The following items are provided in the Management Agent sub-menu for server management:

1. Management Agent Information (see [3.3.1 on page 16](#))

2. Management Blade (see [3.3.2 on page 18](#))

3. System Information (see [3.3.3 on page 19](#))

4. Server Blade (see [3.3.4 on page 20](#))

5. Storage Blade (see [3.3.5 on page 24](#))

6. Connection Blade (see [3.3.6 on page 25](#))

7. User Management (see [3.3.7 on page 26](#))

8. Blue Screen (see [3.3.8 on page 28](#))

9. Event Log (see [3.3.9 on page 29](#))

10. Set System Default (see [3.3.10 on page 30](#))

11. Server Blade CMOS Backup/Restore (see [3.3.11 on page 31](#))

12. Connection Blade Configuration Backup/Restore (see [3.3.12 on page 32](#))

13. Power Consumption (see [3.3.13 on page 33](#))

14. LDAP Authentication (see [3.3.14 on page 34](#))

15. VLAN Information (see [3.3.15 on page 35](#))

16. I2C Bus Management (see [3.3.16 on page 35](#)); no longer available in the sub-menu for server management (as of MMB BX900 firmware version 5.32)
- 17./16. Management Blade Configuration Backup/Restore (see [3.3.17 on page 35](#))
- 18./17. Management Blade Base Configuration Backup/Restore (see [3.3.18 on page 36](#))

3.3.1 Management Agent Information

This item provides several options to configure and display parameters of the management agent, such as the network IP address, Telnet and SMTP parameters, or date and time.

There are options that are used to set a single parameter, while others are used to set more than one. For the former group of parameters their current values are displayed, too.

Altogether, the menu for these options looks like this:

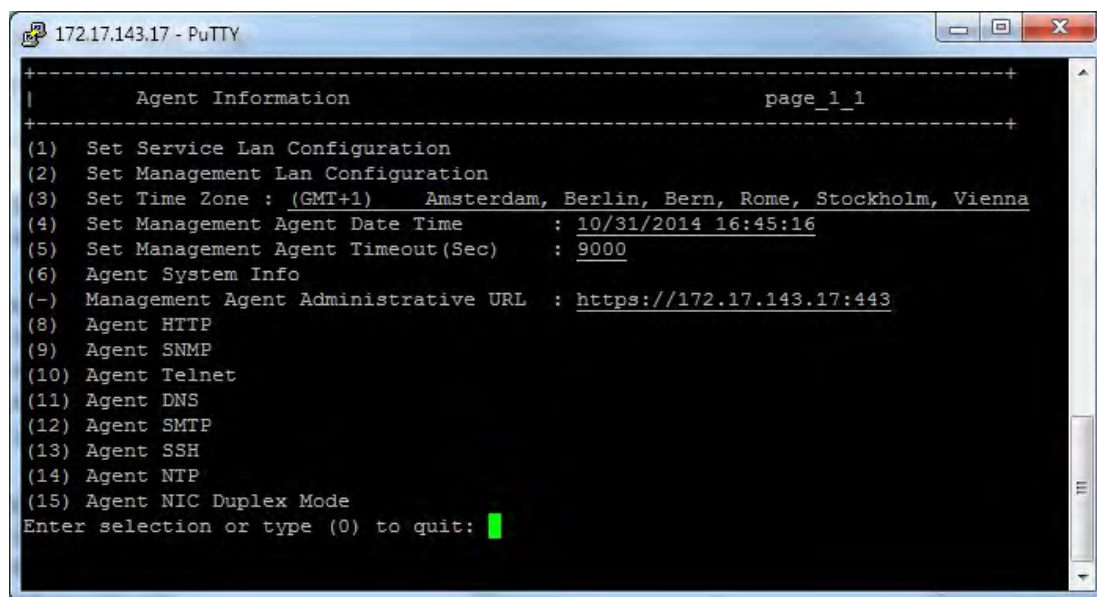


Figure 4: Agent Information menu

These options are used to perform the following activities:

Option	Description
Set Service Lan Configuration	Configuration of the service LAN interface of the MMB.
Set Management Lan Configuration	Configuration of the management LAN interface of the MMB.
Set Time Zone	Configuration of the time zone for the management blade, which is selected from a time zone table.
Set Management Agent Date Time	Configuration of date and time for the management blade.
Set Management Agent Timeout	Configuration of the time-out value for login to the console menu.
Agent System Info	Settings used in SNMP for the management blade: – system name – system location – system contact
Management Agent Administrative URL	Display of the home page URL for the management blade.
Agent HTTP	Configuration of the HTTP settings, including port number assignment, HTTP protocol enabling/disabling and HTTP SSL security control.

Option	Description
Agent SNMP	Configuration of the SNMP settings, including SNMP enabling/disabling, selecting an SMNP community string and a destination from the SNMP trap table.
Agent Telnet	Configuration of the Telnet server settings, including Telnet port assignment and Telnet enabling/disabling.
Agent DNS	Configuration of the DNS server address and enabling/disabling DNS support.
Agent SMTP	Configuration of the SMTP settings for mail sending, including SMTP enabling/ disabling, SMTP sender, SMTP relay server and mail user account.
Agent SSH	Configuration of the SSH settings.
Agent NTP	Configuration of the NTP (network time protocol) service. You can enable or disable the NTP service, set the NTP server's IP address and choose the Sync Mode: – <i>Sync Afterwards</i> Only if the management blade time is behind of NTP server time, the management blade syncs the time from NTP server. – <i>Sync Always</i> The management blade always syncs the time from NTP server, no matter whether the NTP server time is behind or ahead of management blade.
Agent NIC Duplex Mode	Setting of the management blade's NIC duplex mode (<i>full duplex</i> or <i>half duplex</i>). <i>Execution Mode</i> displays the current duplex mode, <i>Setting Mode</i> allows you to specify which duplex mode should be active after the next reset.

3.3.2 Management Blade

Within the blade server management system there are two management blades. One of them is active as the master of the server management system. The other one is in standby mode to ensure the availability of the system.

A number of parameters relating to the management blades is displayed to the user, showing their current values (see next figure):

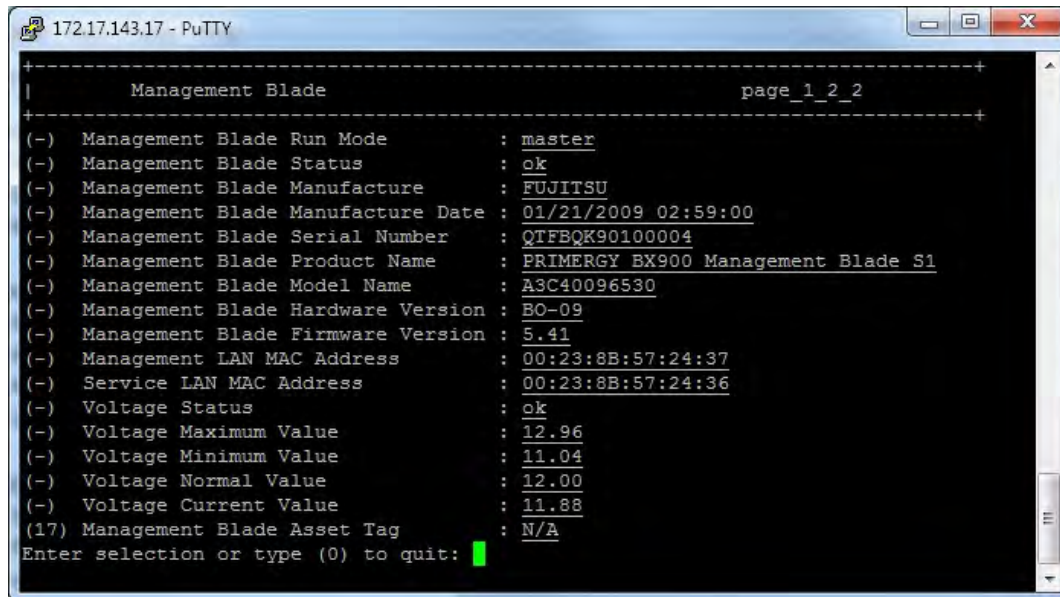


Figure 5: Management Blade menu

The following parameters are displayed:

Parameter	Description
Management Blade Run Mode	Displays whether the management blade is run in master mode or slave (standby) mode.
Management Blade Status	Health status of the management blade. A message will be displayed if this status is disturbed.
Management Blade Manufacture	Name of the manufacturer of the management blade.
Management Blade Manufacture Date	Date of manufacture for the management blade.
Management Blade Serial Number	Serial number of the management blade.
Management Blade Product Name	Product name of the management blade.
Management Blade Model Name	Name of the management blade model.
Management Blade Hardware Version	Hardware version of the management blade.
Management Blade Firmware Version	Firmware version of the management blade.
Management LAN MAC Address	Physical address (MAC address) of the management LAN interface of the MMB.
Service LAN MAC Address	Physical address (MAC address) of the service LAN interface of the MMB.
Management Voltage Status	Status of the voltage supply of the MMB.
Management Voltage Maximum Value	Maximum voltage of the MMB.
Management Voltage Minimum Value	Minimum voltage of the MMB.
Management Voltage Normal Value	Standard voltage of the MMB.
Management Voltage Current Value	Current voltage of the MMB.

Parameter	Description
Management Blade Asset Tag	Sets a unique asset tag for the management blade.

3.3.3 System Information

The System Information option provides information on all components of the blade server management system, such as power supply, fans, temperature, KVM (= keyboard/video/mouse).

The menu for this option looks like this:

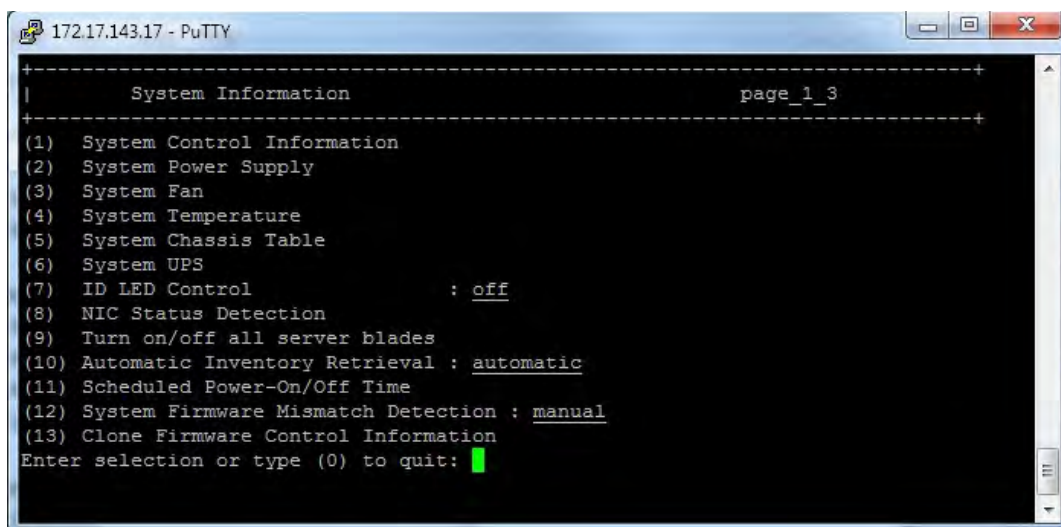


Figure 6: System Information menu

The menu offers the following subordinate options to the user:

Parameter	Description
System Control Information	Displays the number of system fans, power supply groups and temperature sensors, as well as the status of all system components, excepting CPU blades and connection blades.
System Power Supply	Displays information on the power supply units.
System Fan	Displays information on the number and status of the system fans, including parameters like nominal speed, current speed, speed threshold and failure reaction. A fan test is also provided, supporting the fan life time monitor.
System Temperature	Displays information on the system temperature, including current value, warning level, critical level, sensor status and critical temperature reaction.
System Chassis Table	Displays information on the system chassis, including the chassis serial number and if there has been any intrusion into the inside of the chassis.
System UPS	Displays chassis UPS (uninterruptable power supply) information, including UPS number, vendor, type, IP address, connect port, and SNMP community.
ID LED Control	Displays the status of the system control: on, off, or blinking.
NIC Status Detection	In dual MMB mode the roles are switched when the LAN connection to the master fails, and the slave takes over the role of the master.
Turn on/off all server blades	Turns on or turns off all server blades.
Automatic Inventory Retrieval	The function is only working for VIOM. If set to <i>automatic</i> , the inventory retrieval is automatically performed for inserted server blades or when the basic unit is powered on. If set to <i>manual</i> , the automatic inventory retrieval is not done.

Parameter	Description
Scheduled Power-On/Off Time	Configures in detail the power-on/off sequences of the server blades.
System Firmware Mismatch Detection	Used for dual MMB systems, where one MMB firmware version differs from the other. Manual: User has to do the matching by himself after mismatch has been reported. Automatic: After notification of the mismatch the system has to do the matching by starting a firmware flash.
Clone Firmware Control Information	Controls the cloning process of the firmware (in case of mismatch of firmware versions master/slave). 0 = disabled (default).

3.3.4 Server Blade

The Server Blade option provides general information on the server blades, i. e. information on CPUs, memory modules, voltage, temperature, CMOS configuration and watchdog timers.

The menu for this option looks like this:

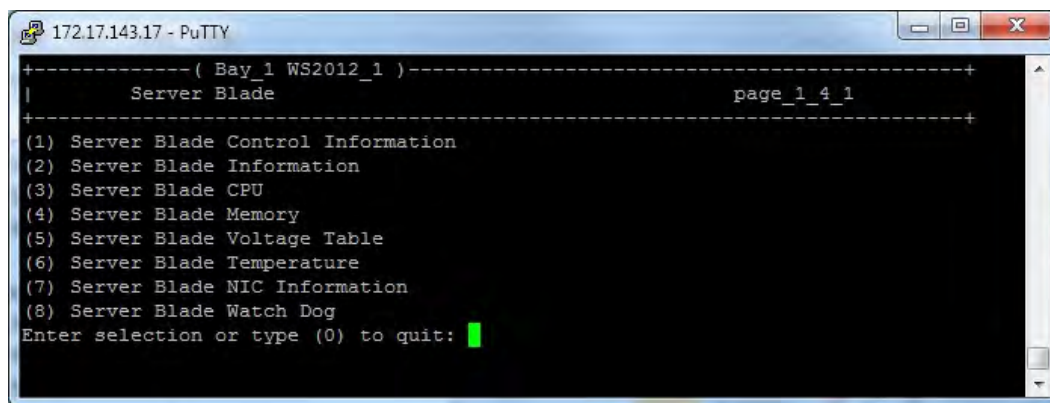


Figure 7: Server Blade menu

3.3.4.1 Server Blade Control Information

This option enables the user to set the following parameters:

Parameter	Description
Server Power	Set server power: (1) on (2) off (3) power-cycle (4) reset (5) NMI (6) force off
Set Server Boot Mode	The boot modes <i>init</i> and <i>inventory</i> are supported by VIOM function. For details, please refer to the VIOM spec.
Set Server Blade Host Name	Host name of the server blade. Is overwritten with the host name assigned in the operating system when ServerView agents are used.
Server LED Control	Configuration of the LED control at the front of the blade server: blinking or off.
Server Memory Dump Flag	Indicates the status of the Server Memory Dump Flag (normal or off).
Server Power On/Off Time Control	The user can set up a power on/off schedule for server blade.

Parameter	Description
Server Power Force Power Off Enabled	Controls the "forced" shutdown (termination of processes is not waited for; these are closed immediately).
Server Power Force Power Off Control	If the "proper" shutdown of the server blade fails, the "forced shutdown" is initiated after <i>n</i> minutes.
BIOS Recovery Flash Bit	This option can be selected if the server blade's BIOS has problems or a flash has failed. After the option has been set, the blade can be started up "without" the BIOS. It then searches autonomously for a suitable BIOS on the connected media (floppy, USB stick, CD/DVD) and flashes it.
iRMC Address Configuration	Sets up the LAN connection of the iRMC.

3.3.4.2 Server Blade Information

This option displays some information on the server blade parameters. The following parameters are included:

Parameter	Description
Server Blade Status	Displays the server blade health status.
Server Blade Manufacture	Displays the server blade manufacturer.
Server Blade Manufacture Date	Displays the server blade production date.
Server Blade Serial Number	Displays the server blade serial number (systems).
Server Blade Identify Serial Number	Displays the server blade serial number (motherboard).
Server Blade Product Name	Displays the server blade product name.
Server Blade Product Version	Displays the server blade product version.
Server Blade Model Name	Displays the server blade model name.
Server Blade Hardware Version	Displays the server blade hardware version.
Server Blade BIOS Version	Displays the server blade BIOS version.
Number of CPU Socket	Displays how many CPU sockets are available on the server blade.
Number of Memory Socket	Displays server blade memory information.
Server Blade OS Type	Displays the OS platform currently running on the server blade.
Server Blade OS Version	Displays the version of the OS currently running on the server blade.
Server Blade iRMC Firmware Version	Displays the server blade iRMC firmware version.
Server Blade Mezzanine Card	Displays whether a Mezzanine card is installed.

3.3.4.3 Server Blade CPU

This option displays some information on the server blade CPU parameters. The following parameters are included:

Parameter	Description
CPU Type	Displays the CPU type.
CPU Frequency	Displays the CPU frequency.
CPU ID	Displays the CPU ID.

Parameter	Description
CPU Status	Displays the CPU status. The values displayed will be: – <i>OK</i> – <i>NOT_PRESENT</i> – <i>ERROR</i> – <i>CRITICAL</i> – <i>MISSING_TERMINATION</i>
CPU Name	Displays the CPU name.
CPU Socket Designation	Displays the CPU socket designation.
CPU Manufacturer	Displays information on the CPU manufacturer.
CPU Clock	Displays the CPU clock.

3.3.4.4 Server Blade Memory

This option provides information on the server blade memory. The information is displayed in two tables:

Table	Description
Server Blade Memory Information Table	Displays information on the total size of the memory, as well as on the error count, the error reset record and the error count start time.
Server Blade Memory Modules Table	Displays the status of each memory module, together with memory type and error information.

3.3.4.5 Server Blade Voltage Table

This option provides information on the server voltage. The following parameters are displayed:

Parameter	Description
Server Voltage Designation	Displays the voltage designation for the server blade.
Server Voltage Status	Displays the voltage status for the server blade. The values displayed will be: – <i>NOT_AVAILABLE</i> – <i>OK</i> – <i>TOO_LOW</i> – <i>TOO_HIGH</i>
Server Voltage Minimum Value	Displays the minimum voltage value for the server blade.
Server Voltage Maximum Value	Displays the maximum voltage value for the server blade.
Server Voltage Current Value	Displays the current voltage value for the server blade.
Server Voltage Nominal Value	Displays the nominal voltage value for the server blade.

3.3.4.6 Server Blade Temperature

This option provides information on the server temperature. Some of the parameters displayed can also be set by the user:

Parameter	Description
Server Temperature Sensor Designation	Displays the designation of the temperature sensor for the server blade.
Server Temperature Sensor Status	Displays the status of the temperature sensor. The values displayed will be: – <i>SENSOR_DISABLED</i> – <i>SENSOR_FAIL</i> – <i>WARNING_TEMP_WARM</i> – <i>CRITICAL_TEMP_WARM</i> – <i>NOT-AVAILABLE</i>
Server Temperature Upper Warning Level	This parameter can be set to configure the upper warning level of the temperature sensor for the server blade.
Server Temperature Upper Critical Level	This parameter can be set to configure the upper critical level of the temperature sensor for the server blade.
Server Temperature Lower Warning Level	This parameter can be set to configure the lower warning level of the temperature sensor for the server blade.
Server Temperature Lower Critical Level	This parameter can be set to configure the lower critical level of the temperature sensor for the server blade.
Server Temperature Current Value	Displays the current temperature value for the server blade.

3.3.4.7 Server Blade NIC Information

This option displays the IP and MAC address of the server blade.

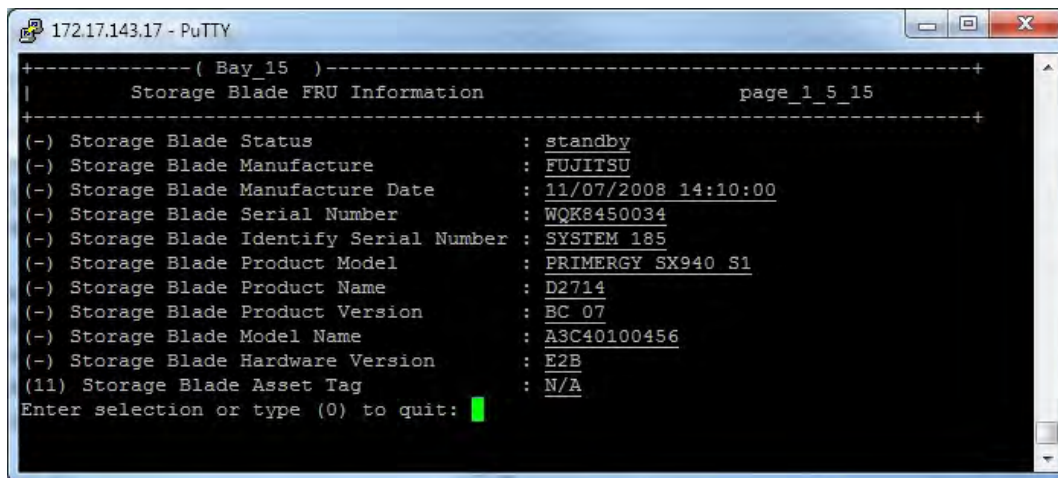
3.3.4.8 Server Blade Watch Dog

This option is used to configure the watchdog timers for the server blade. There are two timers that can be set here:

Timer	Description
Server Blade Software Watchdog	This timer is used to monitor the operation system and the software applications. A watchdog timer agent that resets the timer must be implemented in the operation system. When the time-out is reached, a time-out routine will be started.
Server Blade Boot Watchdog	This timer is used to monitor the server blade POST. It will be reset by the BIOS in periods configured within the POST code. When the time-out is reached, a time-out routine will be started.

3.3.5 Storage Server Blade

The menu for this option looks like this:



```

172.17.143.17 - PuTTY
+------( Bay_15 )-----+
|      Storage Blade FRU Information      page_1_5_15
+-----+
(-) Storage Blade Status           : standby
(-) Storage Blade Manufacture      : FUJITSU
(-) Storage Blade Manufacture Date  : 11/07/2008 14:10:00
(-) Storage Blade Serial Number    : WQK8450034
(-) Storage Blade Identify Serial Number : SYSTEM 185
(-) Storage Blade Product Model    : PRIMERGY SX940 S1
(-) Storage Blade Product Name     : D2714
(-) Storage Blade Product Version  : BC 07
(-) Storage Blade Model Name       : A3C40100456
(-) Storage Blade Hardware Version  : E2B
(11) Storage Blade Asset Tag       : N/A
Enter selection or type (0) to quit:

```

Figure 8: Storage Server Blade menu

The following parameters are displayed:

Parameter	Description
Storage Blade Status	Displays the storage blade health status.
Storage Blade Manufacture	Displays the storage blade manufacture vendor.
Storage Blade Manufacture Date	Displays the storage blade manufacture date.
Storage Blade Serial Number	Displays the storage blade serial number (systems).
Storage Blade Identify Serial Number	Displays the storage blade serial number (motherboard).
Storage Blade Product Model	Displays the type name of the storage blade (e.g. PRIMERGY SX940 S1).
Storage Blade Product Name	Displays the storage blade product name.
Storage Blade Product Version	Displays the storage blade product version.
Storage Blade Model Name	Displays the storage blade model name.
Storage Blade Hardware Version	Displays the storage blade hardware version.
Storage Blade Asset Tag	Sets a unique asset tag for the storage blade.

3.3.6 Connection Blade

The Connection Blade option is used to display information on the connection blades that are part of the blade server system.

Currently supported are the following types of connection blades:

- GbE (Ethernet) Connection Blade
- Ethernet Pass Thru Connection Blade
- SAS Connection Blade
- FC Connection Blade
- FC Pass Thru Connection Blade
- InfiniBand Connection Blade
- Brocade VDX 2730 Connection Blade
- Cisco Nexus B22 Connection Blade

The menu for all these types is the same and looks like this:

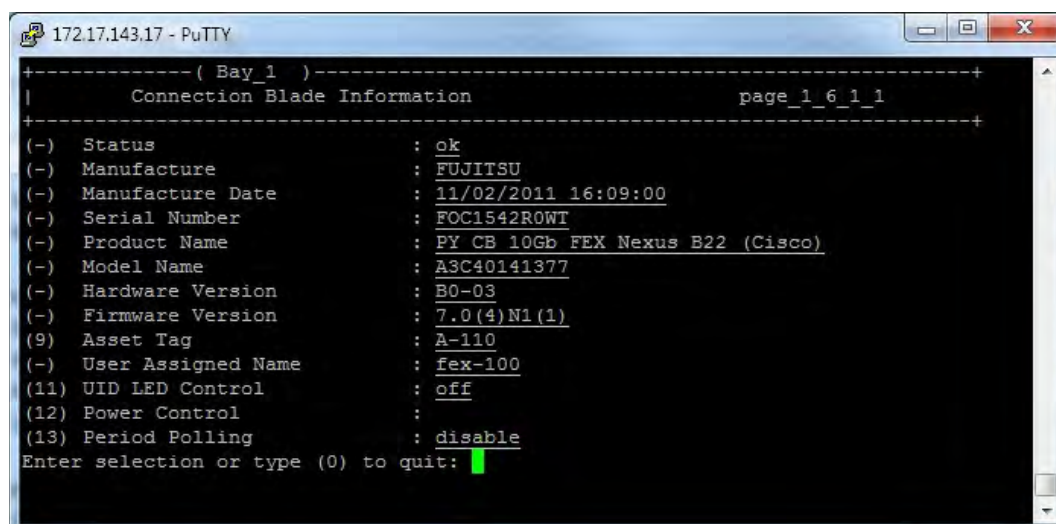


Figure 9: Connection Blade menu

The following parameters are displayed:

Parameter	Description
Status	Displays the status. This status can be retrieved by the management blade via a CLI command.
Administrative URL	The URL at which the MMB can be reached using a Web browser.
Manufacture	Displays information on the manufacturer.
Manufacture Date	Displays the manufacturing date.
Serial Number	Displays the serial number.
Product Name	Displays the product name.
Model Name	Displays the model name.
Hardware Version	Displays the hardware version.
Firmware Version	Displays the firmware version.
Asset Tag	Sets a unique asset tag for the connection blade
User Assigned Name	The name of the connection blade (can be assigned by the user).
UID LED Control	Sets the LED off or blinking.

Parameter	Description
Power Control	Starts rebooting the connection blade.
Refresh	Enables/disables the refresh function.
Connection Blade Mode	GbE connection blades can run in two different modes – Switch and IBP. The mode enabled is displayed here.
Reset Interface Settings	Sets the configuration settings to default.
Stacking State	Applies for Connection Blade GbE Switch/IBP 36/8+2 (SB11). These can be interconnected to form a stack. Possible state: Master or Member.
Inter-Switch Link Setting	Applies for Connection Blade GbE Switch/IBP 36/8+2 (SB11). Two SB11s which are operated in a fabric (horizontally adjacent to each other) can be interconnected to form "one" connection blade. A common management interface then exists for the connected connection blades.

3.3.7 User Management

The User Management option is used to change, add and delete users.

The following four user types (roles) with different permission rights are possible:

1. Administrator
2. OEM
3. Operator
4. User

The access rights of the various user roles are as follows:

Administrator

This role allows the user

- to create, update, and delete a user account
- to configure system settings related to the MMB, connection blades, and server blades
- to use commands on the iRMC controller as a result of IPMI permission level assignments of LAN/Serial for administrators
- to use the functions at the usual user interfaces (Web UI, CLI etc.)

OEM

This role allows the user

- to have the same functions as the Administrator and
- to use OEM commands and functions on the iRMC controller

Operator

This role allows the user

- to use commands on the iRMC controller as a result of IPMI permission level assignments of LAN/Serial for operators
- to use the functions at the usual user interfaces (Web UI, CLI etc.)

User

This role allows the user

- to use the functions at the usual user interfaces (Web UI, CLI etc.)

Example: Deleting a user

The methods for creating a new user or changing a user name or rights are intuitive and present no problems. The situation is somewhat different when an existing user is to be deleted, because no explicit entry is provided for this. We will therefore use an example to describe how you must proceed in this case.

Step 1

Select the user to be deleted, in this example the user *Tom* – type 2:

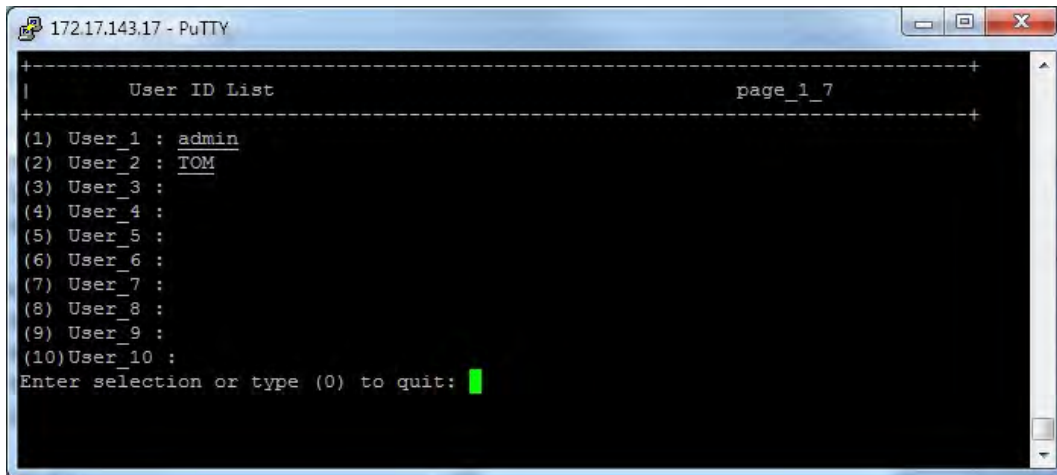


Figure 10: User Management – deleting a user

Step 2

Now select the name of the user to be deleted – type 1:

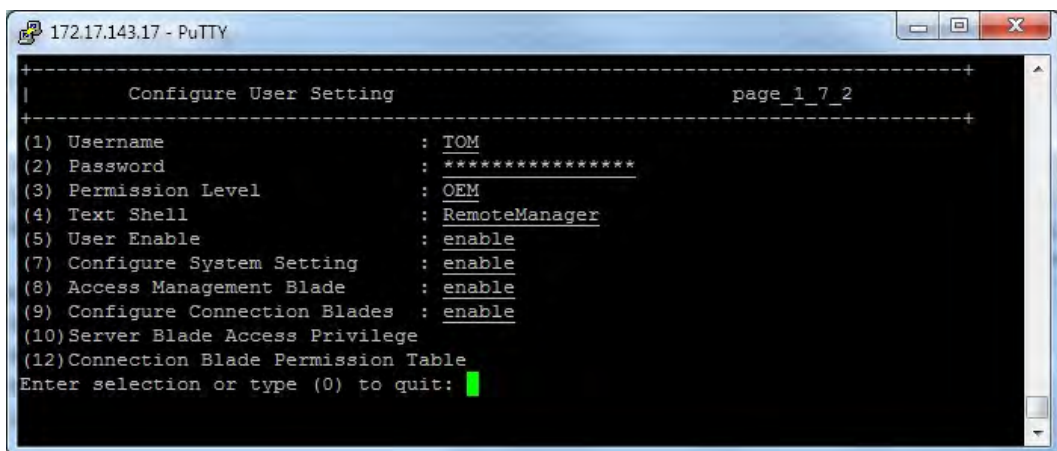


Figure 11: User Management – deleting a user

Step 3

To delete the user, simply press the space bar:

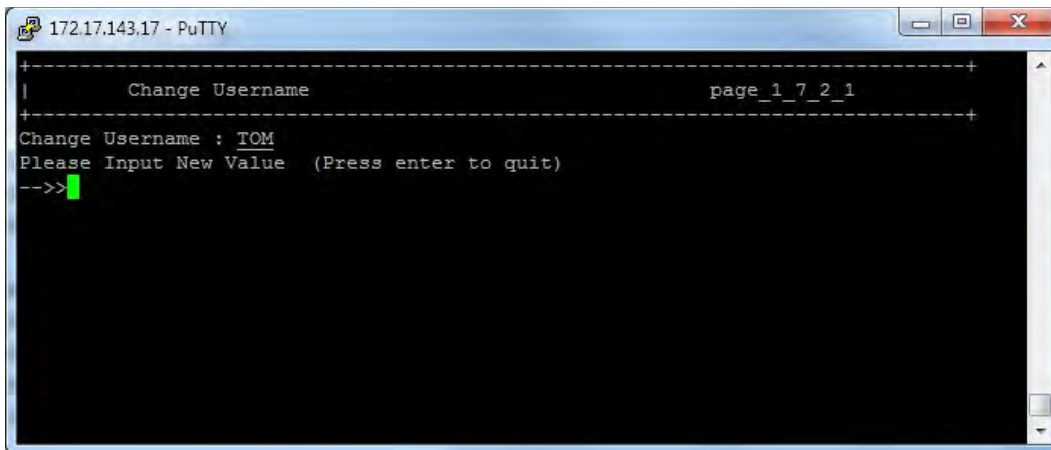


Figure 12: User Management – deleting a user

Step 4

User *Tom* has been deleted, as you can see in the menu:

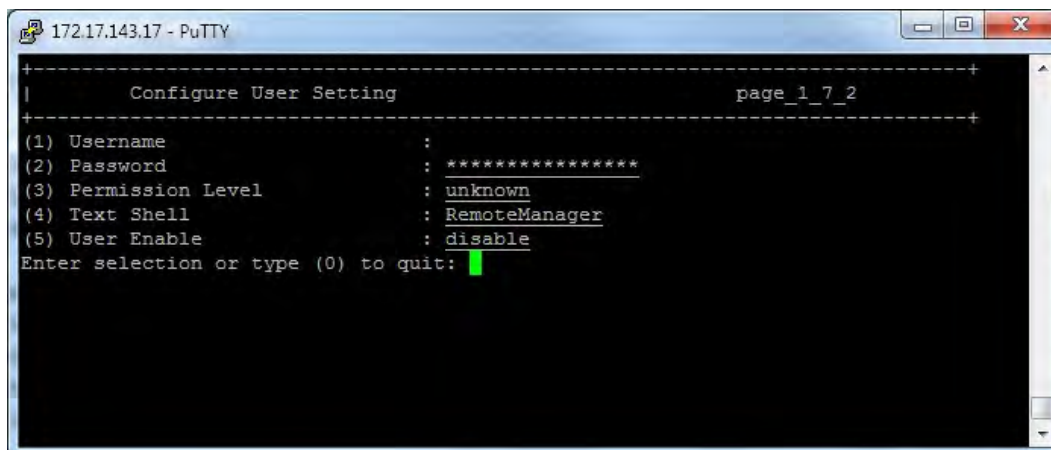


Figure 13: User Management – deleting a user

3.3.8 Blue Screen

The Blue Screen option is available, if the operating system used supports the blue screen feature, as provided by UART.

The option will then display which server blades are currently in blue screen status.

3.3.9 Event Log

The Event Log option is used to display the events that have been logged on the management blade and the server blades.

The menu for this option looks like this:

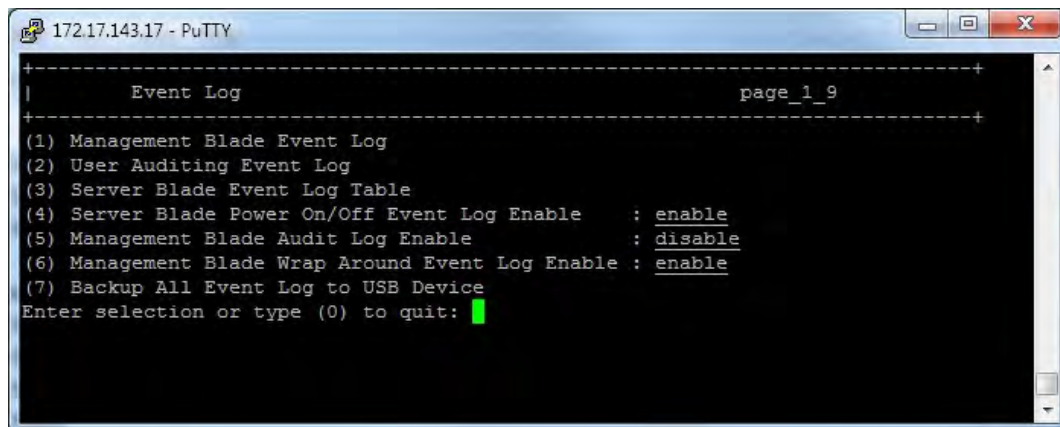


Figure 14: Event Log menu

Information is displayed for:

- Events that were logged on the management blade event log
- Events that were logged on a server blade event log

3.3.9.1 Management Blade Event Log

This sub-option is used to display the events that have been logged on the management blade event log.

The following parameters are displayed:

Parameter	Description
All Event	All events that have been logged on the management blade.
Informational Event	The informational events that have been logged on the management blade.
Minor Event	The minor events that have been logged on the management blade.
Major Event	The major events that have been logged on the management blade.
Critical Event	The critical events that have been logged on the management blade.
Clear All Entries	This parameter is used to clear all events from the management blade event log.

3.3.9.2 Server Blade Event Log Table

This sub-option is used to display the events that have been logged on a server blade event log.

After a server blade has been selected, the following parameters are displayed:

Parameter	Description
All Event	All events that have been logged on the server blade.
Informational Event	The informational events that have been logged on the server blade.
Minor Event	The minor events that have been logged on the server blade.
Major Event	The major events that have been logged on the server blade.
Critical Event	The critical events that have been logged on the server blade.
Clear All Entries	This parameter is used to clear all events from a server blade event log.

3.3.9.3 Server Blade Power On/Off Event Log Enable

This option is used to specify, whether power on/off events for the server blades should be listed in the event log.

3.3.9.4 Management Blade Wrap Around Event Log Enable

This option is used to specify whether the wrap-around functionality for the event log should be used or not.

Parameter	Description
enable	When the event log repository is full, new event log entries replace the old ones beginning with the first event log entry.
disable	When the event log repository is full, no event log entries are written any longer.

3.3.9.5 Backup All Event Log to USB Device

This option is used to save the MMB's event log to a USB medium.

Parameter	Description
USB device selection	Selects the USB medium (all the devices connected to the MMB are displayed here).
Filename (empty default name)	Name of the file which will be written to USB – if nothing is entered, a default name is used.
Enable	Starts the backup to the USB medium.

3.3.9.6 Management Blade Wrap Around Event Log Enable

Specifies whether the wrap-around functionality of the event log should be used or not.

Enabled (= 1): When the event log repository is full, new event log entries replace the old ones beginning with the first event log entry.

Disabled (= 0): When the event log repository is full, no event log entries are written any longer.

3.3.9.7 Backup All Event Log to USB Device

BX400 only. Copies the log message to USB device. 0 = disabled.

3.3.10 Set System Default

The Set System Default option is used to restore the default values.

The menu for this option looks like this:

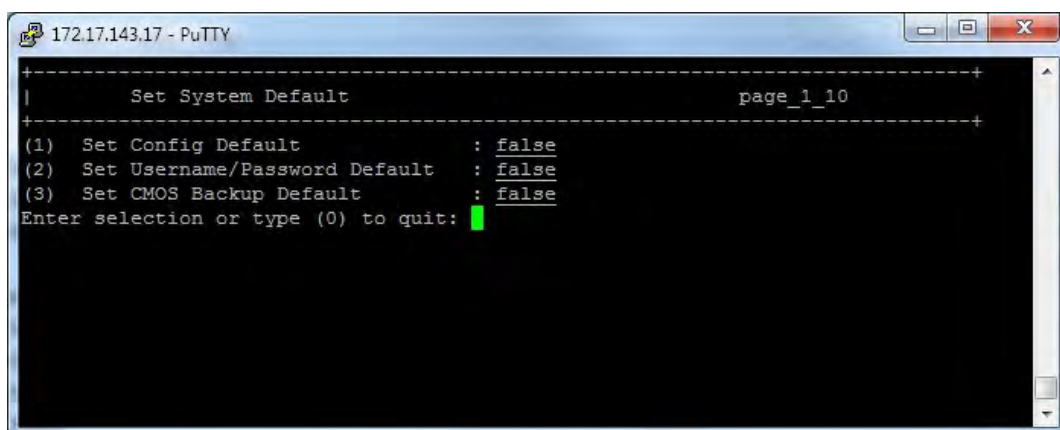


Figure 15: Set System Default menu

The following parameters can be set:

Parameter	Description
Set Config Default	The configuration of the management blade is set to the default values.  Please note that all configured values are lost and the management blade has to be configured newly after using this option.
Set Username/Password Default	All configured user names with the exception of <i>admin</i> are deleted. The password for the user <i>admin</i> is set to the default (" <i>admin</i> ").
Set CMOS Backup Default	All connection blade configuration backups and all server blade BIOS backups are deleted.

3.3.11 Server Blade CMOS Backup/Restore

 This function supports S1 and S2 server blades only.

This option is used to backup and restore server blade BIOS parameters. The server blade must be powered on before backup/restore processing. If the backup is successful, the backup file will be displayed in the CMOS backup file table.

After selecting the server blade whose BIOS is to be backed up or whose backup file is to be restored, the *Server CMOS Configure* option is displayed:

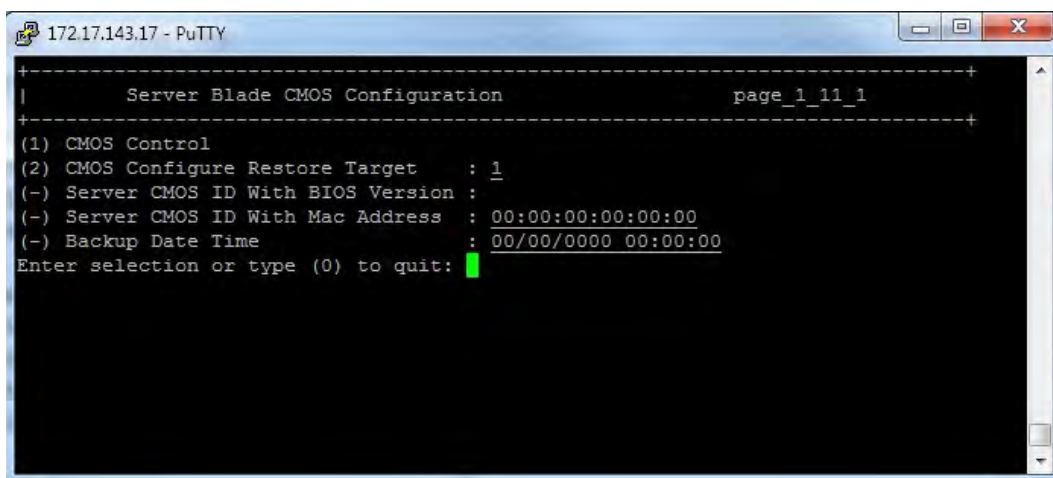


Figure 16: Server CMOS Configure menu

The following parameters are displayed:

Parameter	Description
CMOS Control	Specifies the backup/restore policy: <i>backup</i> The BIOS parameters of the selected server blade are backed up. <i>smart-restore</i> After the slot id, BIOS version and MAC address have been verified, the backup file of the selected server blade is restored. <i>force-restore</i> The backup file is restored without verification.
CMOS Configure Restore Target	Specifies the server blade whose BIOS parameters are to be restored.
Server CMOS ID With BIOS Version	Displays the CMOS ID with BIOS version.
Server CMOS ID With Mac Address	Displays the CMOS ID with MAC address
Backup Date Time	Displays date and time of the backup file generation.

3.3.12 Connection Blade Configuration Backup/Restore

This option is used to backup/restore the configuration values of the connection blade.

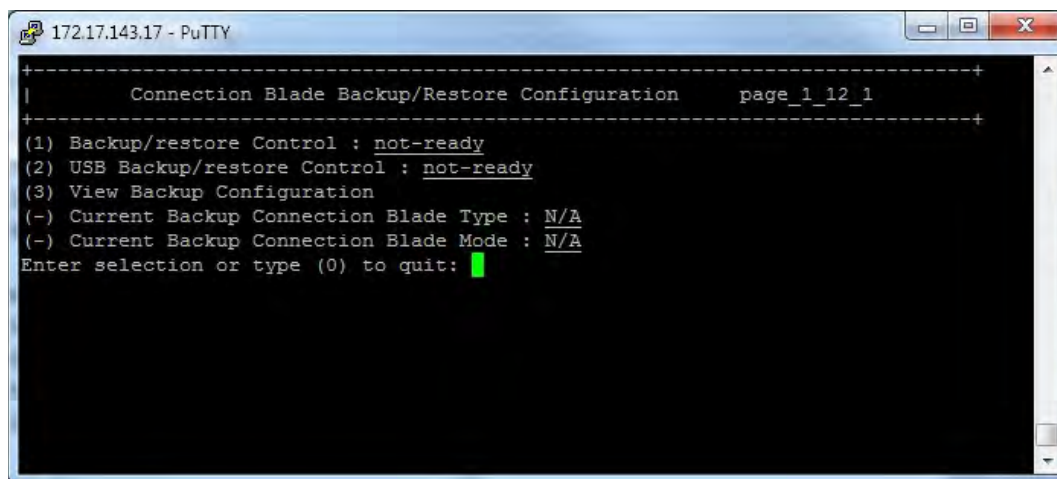


Figure 17: Connection Blade Configuration Backup/Restore

The following parameters are displayed:

Parameter	Description
Backup/restore Control	Specifies whether a backup process or a restore process is to be started.
USB Backup/restore Control	Specifies whether a backup process or a restore process for a USB medium is to be started.
View Backup Configuration	Displays the configuration of the connection blade when a backup has been saved successfully.
Current Backup Connection Blade Type	Displays the type of connection blade (SB11/SB11a, etc.) when a backup has been saved successfully.
Current Backup Connection Blade Mode	Displays the mode of the connection blade (Switch Mode, IBP) when a backup has been saved successfully.

3.3.13 Power Consumption

This option is used to control the power consumption.

The menu for this option looks like this:

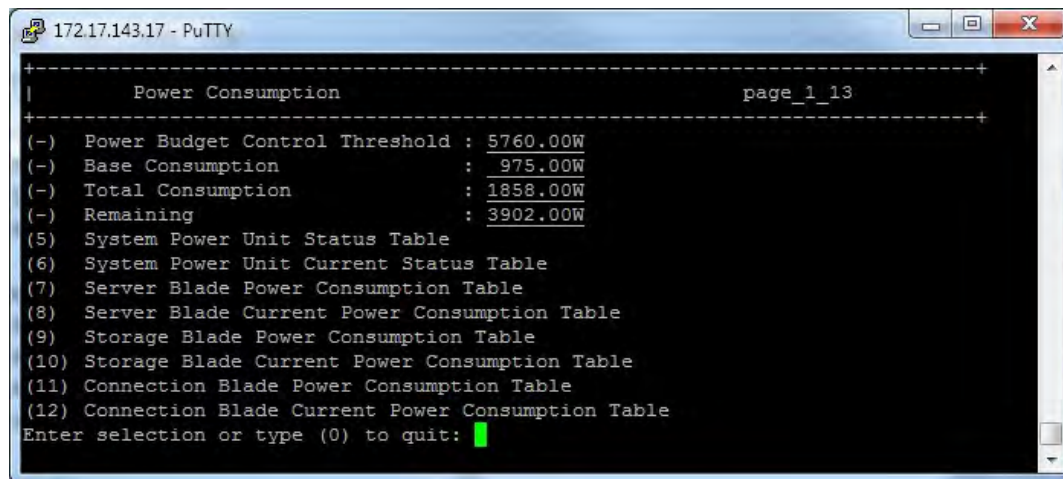


Figure 18: Power Consumption menu

The following parameters are displayed:

Parameter	Description
Power Budget Control Threshold	Displays the max. DC power of the active power supply.
Base Consumption	Power consumption of the base system. Includes one management blade and 6 fan modules.
Total Consumption	Current power consumption of the whole blade server system (including server blades).
Remaining	Difference between <i>Power Budget Control Threshold</i> and current <i>Total Consumption</i> .
System Power Unit Status Table	Displays the max. DC power and the voltage range of the power supply units.
System Power Unit Current Status Table	Displays the current status of each active PSU (power consumption and voltage).
Server Blade Power Consumption Table	Displays the max. DC power consumption of each server blade.
Server Blade Current Power Consumption Table	Displays the current status of each active server blade (power consumption).
Storage Blade Power Consumption Table	Displays the max. DC power consumption of each storage blade.
Storage Blade Current Power Consumption Table	Displays the current status of each active storage blade (power consumption).
Connection Blade Power Consumption Table	Displays the max. DC power consumption of each connection blade.
Connection Blade Current Power Consumption Table	Displays the current status of each active connection blade (power consumption).
Set Power Budget Control (no longer available as of firmware version 5.32)	Settings for power control (redundancy, dynamic, limit values, etc.) – observe submenus.

3.3.14 LDAP Authentication

Use LDAP to login to the MMB through the Web-based or a CLI interface. The login syntax is: *username@domain* (where *username* is an ASCII string of 1-256 bytes).

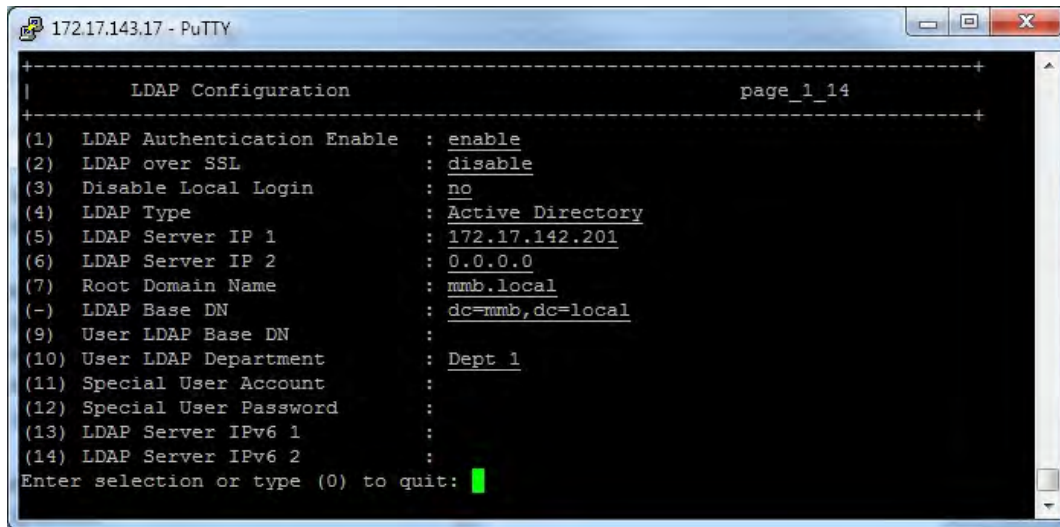


Figure 19: Active Directory Authentication menu

The following parameters are displayed:

Parameter	Description
LDAP Authentication Enable	Enables/disables the LDAP functionality.
LDAP Type	Selects the LDAP type (Microsoft's Active Directory, OpenLDAP, Novell's eDirectory).
LDAP over SSL	Selects whether LDAP is to use a secure SSL connection.
LDAP Server IP 1/2	IP addresses of the primary and, if present, secondary LDAP server.
Root Domain Name	Name of the domain in which the user logs in.
User LDAP Base DN	<i>Distinguished Name</i> , a unique object name in LDAP directories.
User LDAP Department	"Department" of the user in the LDAP directory.
Special User Account	Needed to set up a connection to the LDAP server.
Special User Password	Password for setting up a connection to the LDAP server.

3.3.15 VLAN Information

MMB supports up to 10 VLAN IDs and as of MMB BX900 firmware version 4.71 27 VLAN IDs. In a BX400 the MMB supports up to 13 VLAN IDs.

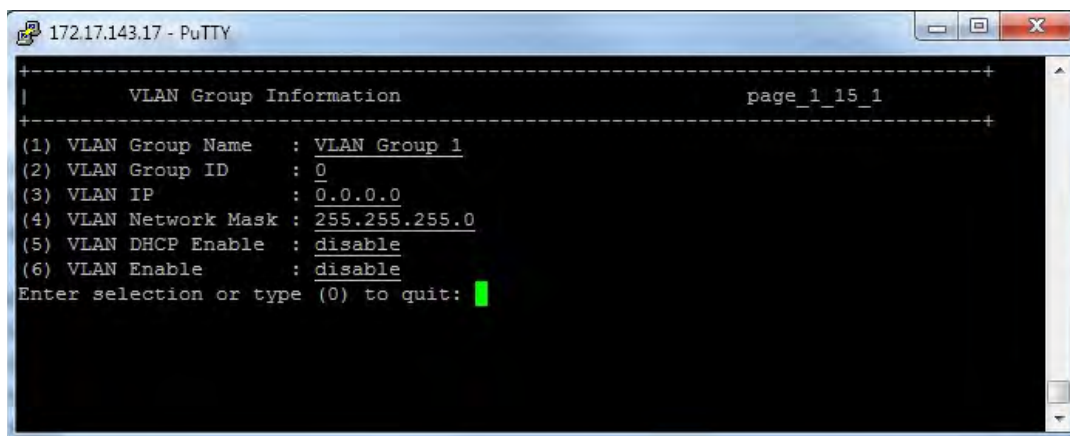


Figure 20: VLAN Information menu

The following parameters are displayed for each group:

Parameter	Description
VLAN Group ID	Identifies different VLAN group IDs. The integer 2 to 4095 are supported.
VLAN IP	Sets the VLAN IP.
VLAN Network Mask	Sets the VLAN network mask.
VLAN Enable	Enables/disables the VLAN function.
VLAN IPv6	The menu item is no longer available as of MMB BX900 firmware version 4.71.

3.3.16 I2C Bus Management



This function is no longer available in the sub-menu as of MMB BX900 firmware version 5.32.

3.3.17 Management Blade Configuration Backup/Restore

This option enables all the MMB settings, including certificates, users, etc., to be backed up/restored.

The menu for this option looks like this:

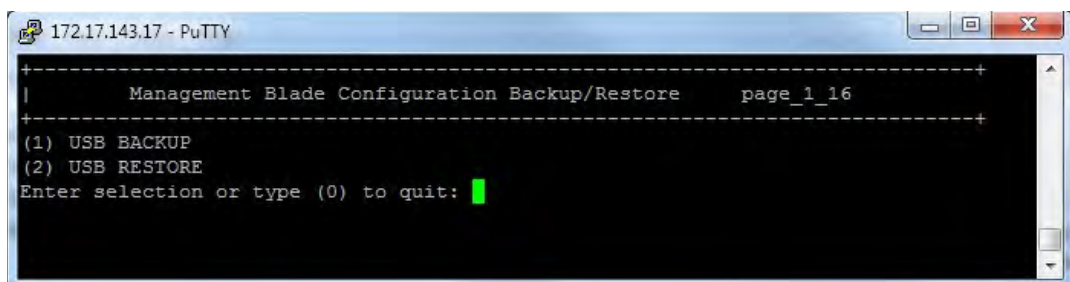


Figure 21: Management Blade Configuration Backup/Restoration menu

3.3.18 Management Blade Base Configuration Backup/Restore

This option enables the most important MMB settings (Language, Identification, Network, Power Settings, PIN Settings) to be backed up/restored.

The menu for this option looks like this:

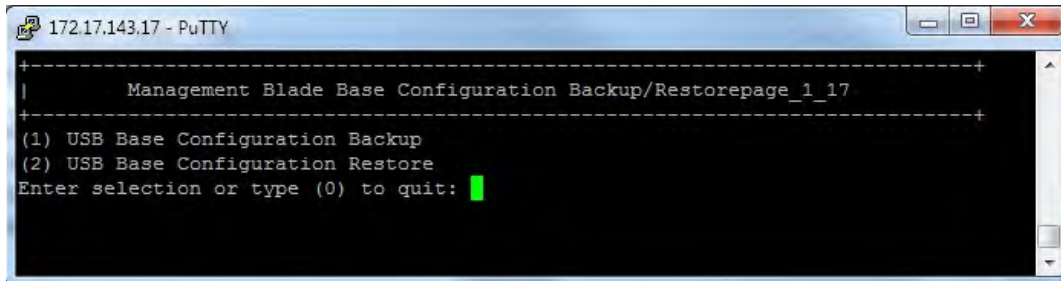


Figure 22: Management Blade Base Configuration Backup/Restoration menu

3.4 Emergency Management Port

The Emergency Management Port (EMP) is for internal use only!

The starting page for these option looks like this:

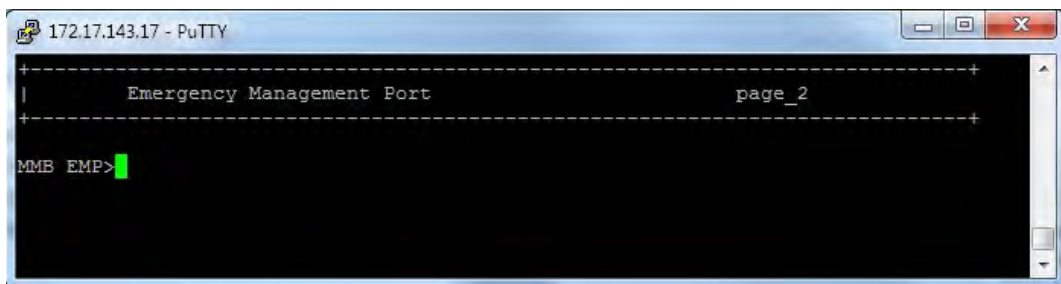


Figure 23: Starting page for Emergency Management Port option



Type A plus <enter> to quit the EMP.

3.5 Console Redirection

There is one console port (serial port interface) within the blade server system. Console redirection can be configured for server blades or connection blades.

The menu for this option looks like this:

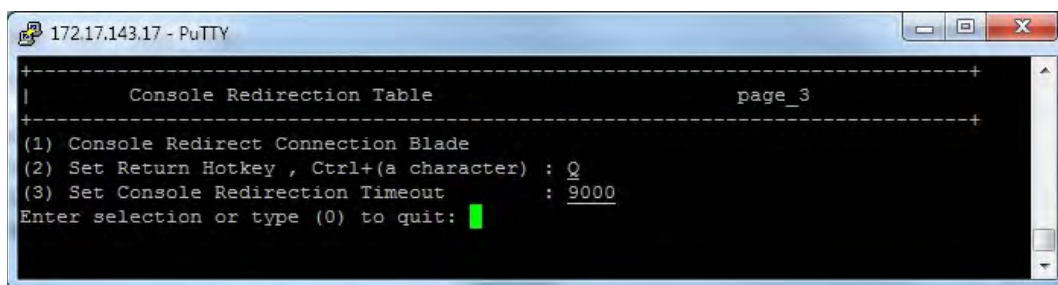


Figure 24: Console Redirection menu

There is a sub-option of console redirection for server blades and one for connection blades. Furthermore, a return hotkey can be configured:

Sub-option	Description
Console Redirect Connection Blade	This option is used to configure a connection blade for console redirection.
Set Return Hotkey, Ctrl+(a character)	This option is used to configure a return hotkey. To do this, a character from A-Z is chosen, excluding M. The hotkey to exit console redirection and return to the previous mode is then Ctrl + the character that has been set here, e.g. Ctrl + R. The default character used for the return hotkey is Q.
Set Console Redirection Timeout	An active connection is automatically disconnected after <i>n</i> seconds.

3.6 TFTP Update

The TFTP Update option is used to perform an update of the management blade firmware.

 For further information on updating BX components please refer to the Operating Manual of your BX system.
The menu for this option looks like this:

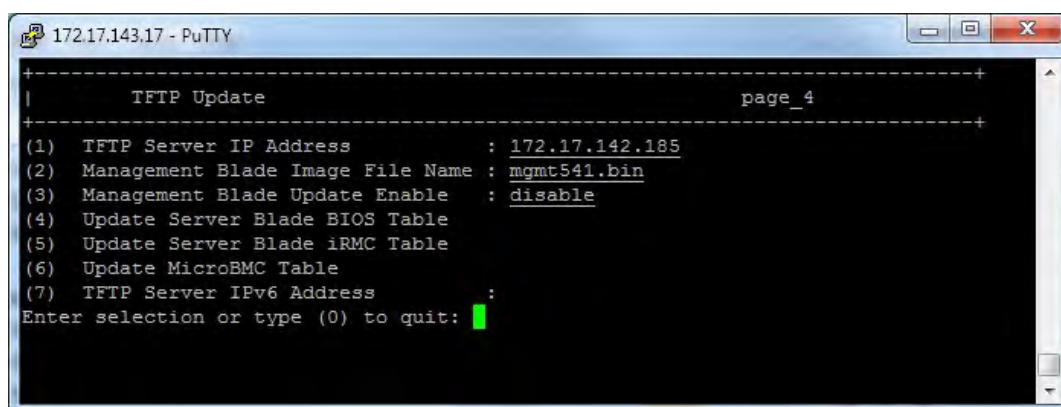


Figure 25: TFTP Update menu

The following parameters can be set:

Parameter	Description
TFTP Server IP Address	Setting of an IP address for the TFTP server.
Management Blade Image File Name	Setting of a file and path name for the management blade image.
Management Blade Update Enable	Upgrading of the management blade firmware. The default value for this parameter is disable. After setting the parameter to enable, the TFTP server must be started, and the management blade must be rebooted. The update will then be performed as the system powers up.
Update Server Blade BIOS Table	Upgrading of the Server Blade BIOS. This option is used to enable/disable the update and to display the TFTP status.
Update Server Blade iRMC Table	Upgrading of the Server Blade iRMC firmware. This option is used to enable/disable the update and to display the TFTP status.
Update MicroBMC Table	Upgrading of the Server Blade MicroBMC firmware. This option is used to enable/disable the update and to display the TFTP status (SX960 and SX980 only).
TFTP Server IPv6 Address	Setting of an IPv6 address for the TFTP server.

3.7 Logout

This option is provided to perform a logout from the Telnet console menu.

3.8 Change Management Role To Slave

This item is used to change the management blade role from master to slave.

3.9 System Information Dump

This option is used to display the event logs of management blades or server blades and to display consecutive lists of configuration/status information. The menu for this option looks like this:

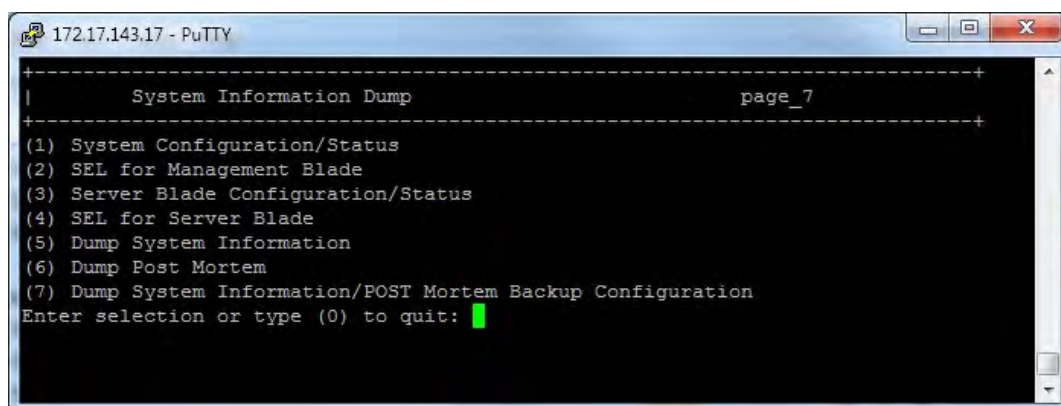


Figure 26: System Information Dump menu

The following parameters are displayed:

Parameter	Description
System Configuration/Status	Displays a consecutive list of system information, e.g. status, IP address, MAC address and firmware version of the connection blades.
SEL for Management Blade	Displays the management blade event log.
Server Blade Configuration/Status	Displays a consecutive list of information about the server blades, e.g. status, BIOS version, iRMC firmware version, OS type and OS version.
SEL for Server Blade	Displays the server blade event log.
Dump System Information	Provides information about temperatures, voltages, fan speeds, all modules' FRU data and event logs.
Dump Post Mortem	Use in case of problem, to get all necessary information on customer site to analyze the problem in the development.
Dump System Information/POST Mortem Backup Configuration	Permits the System Information Dump and POST Mortem Dump to be backed up on a USB medium.

3.10 Command Line Interface

This option is used to get chassis information or to manage series of servers.

The menu for this option looks like this:

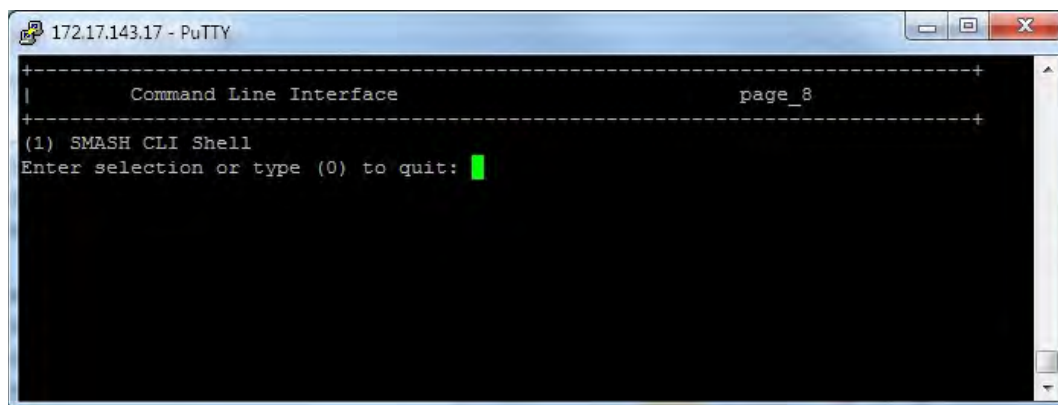


Figure 27: Command Line Interface menu

The following parameters are displayed:

Parameter	Description
SMASH CLP Shell	The SMASH (Systems Management Architecture for Server Hardware) Shell enables a simple and intuitive management of servers in data centers independent of machine state, operating system state, server system topology or access method.



You find the documentation of the SMASH CLP Shell in the MMB Web User Interface help pages:

1. Click the *Help* field at the far right below the Fujitsu logo.
 2. Click *On Contents*.
 3. Navigate to section *Available Help Texts, Notes*.
 4. In the *OEM SM CLP targets and concept* item, click *concept* to open an introduction and *targets* to see details.
- Type *exit* to quit the SMASH CLP submenu.

3.11 Account Management

This option is used to change the user password. The menu for this option looks like this:

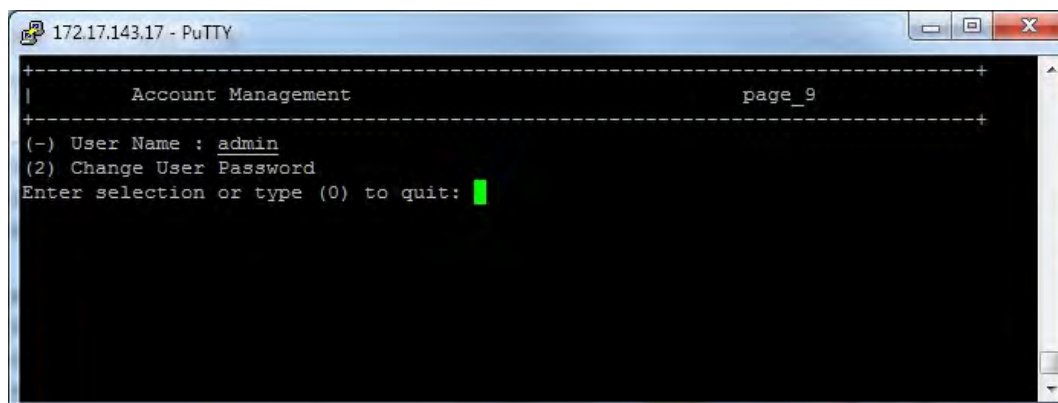


Figure 28: Account Management menu

4 Web User Interface

On the web server an interactive and user-friendly web user interface, known as web console, is provided for server management. It does not depend on any special operating system for a platform. You log into this interface via the web browser.

4.1 Login

You log into the web server by entering an IP address in the browser's URL line, e.g.

`http://10.40.36.185` (example for a management blade address)

- Default IP address: 192.168.1.10
- HTTP SSL disabled: Port 80
- HTTP SSL enabled: Port 443
- Supported Web browsers: Internet Explorer and Firefox (always the current and the antecessor version)
- Maximum number that can be connected at the same time:
 - Telnet: 4
 - SSH: 4
 - http/https: 10

A pop-up window will then open in which you enter your user name and password:



Figure 29: Input mask for login (Internet Explorer)

The default user name and the default password are both *admin*.



If you enter an incorrect password more than three times, the message *No Access Right!* will appear.

4.2 The Start Page

After you have logged in successfully, a home page (start page) is displayed which provides an overview of the system configuration, i.e. the installed components and their current status. The start page looks like this:

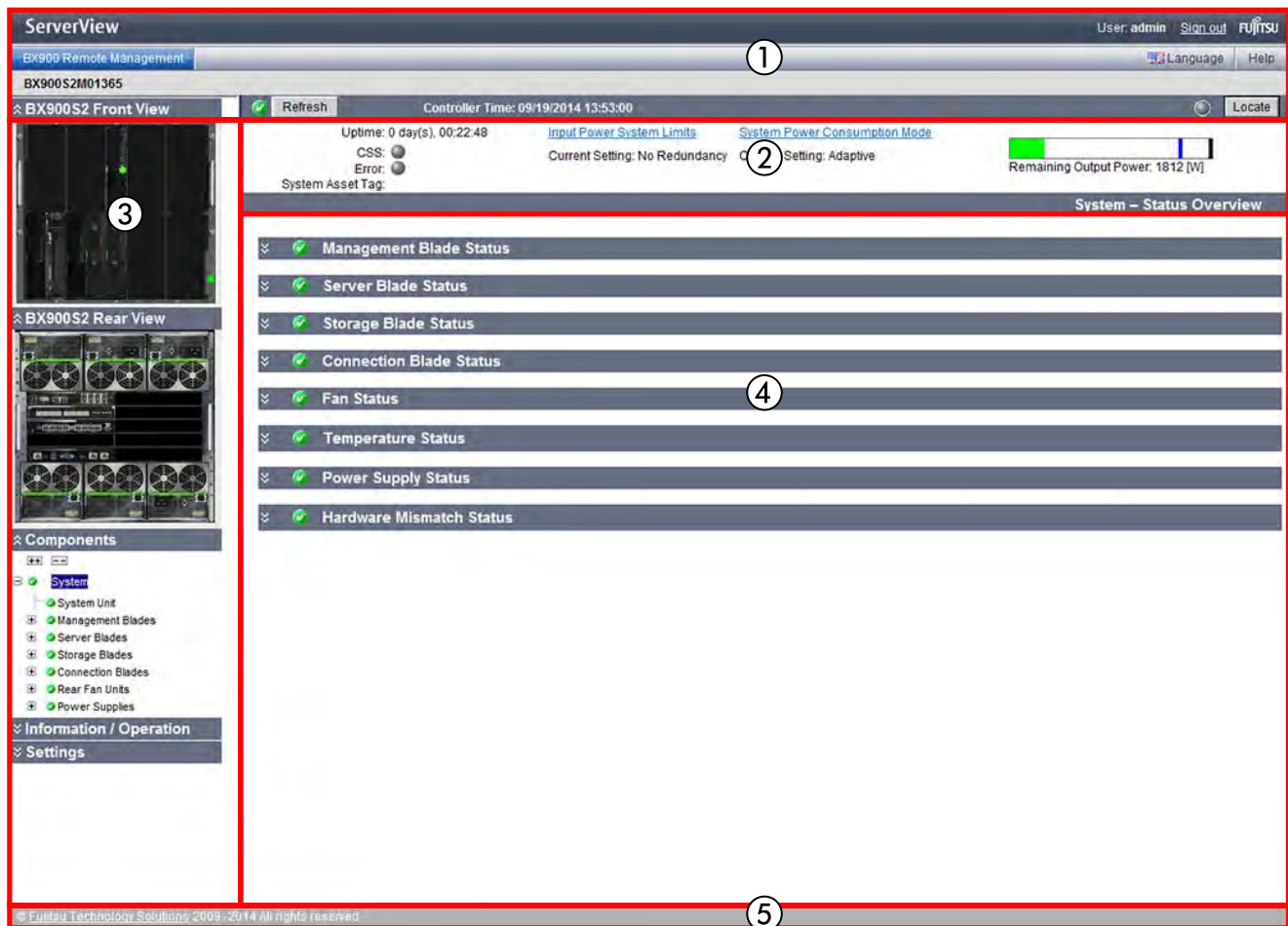


Figure 30: Frames of the start page

The start page consists of five frames:

banner frame (1), status frame (2), navigation frame (3), main frame (4) and bottom frame (5).

1. Banner frame (1)

The banner frame comprises the following fields:

- The name of the blade server (in this example a BX900 system unit) is displayed in the field on the left below the ServerView logo.
- The name of the current user (in this example the user *admin*) is displayed in the upper field on the right.
- A link for signing out (*Sign out*) beside the name of the user who is currently logged in.
- A *HELP* field at the far right below the Fujitsu logo.

The *HELP* field is in turn subdivided into three fields. These fields become visible as soon as the cursor points to *HELP*. The fields are:

- *About*
Supplies information about the current firmware status.
- *On Page*
Shows the help text for the selected menu item (see *Navigation frame* below).

- *On BX900 Remote Management*
Supplies an overview of all help texts.

The banner frame is collapsible (☐).

2. Status frame (2)

The status frame consists of a number of graphical or text controls or displays. Taking our example in [figure 30](#), we will describe the various elements below, showing the graphical elements in a list and separating them with |. Viewed from top left to bottom right, the following elements are involved here:



This field displays the overall status of the blade server.

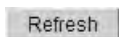
The icon on the left (red) indicates that an error of the type "Critical Error" has occurred in the system. Such as error must be corrected immediately. The components which are affected are displayed in the navigation frame (see below). It is possible for more than one error of this type to occur in the system.

The icon in the middle (yellow) indicates that an error of the type "Warning" or "PDA Error" has occurred in the system. A PDA (Prefailure Detection Analysis) reports problems in hardware components (fans, CMOS batteries, memory modules and hard disk drives) *before* these result in a system failure. The component which is affected is displayed in the navigation frame (see below). It is possible for more than one error of this type to occur in the system.

The icon on the right (green) indicates that the system is operating without error.



If errors of the type "Critical Error" and of the type "Warning" or "PDA Error" have occurred simultaneously in the system, the *higher-ranking* error, i.e. the red icon, is always displayed here.



This button enables you to refresh all the blade server data.

Uptime

Specifies the time since the blade server was started.

CSS:  | *yellow blinking* | 

This field indicates errors of the type "CSS" (Customer Self Service), in other words errors which users can rectify themselves. The component which is affected is displayed in the navigation frame (see below).

The *yellow* icon indicates that an error of the type "Warning" or "PDA Error" has occurred in the system. When the yellow icon is in the *blinking* state, it is not a warning but indicates an error of the type "Critical Error". Detailed information on these error types is provided at the start of this list. The *gray* icon indicates that all system components are operating without error.

Error:  | *red blinking* | 

This field indicates errors of the type "Error", in other words errors which *cannot* be corrected by the user, but can only be rectified by Customer Service. The component which is affected is displayed in the navigation frame (see below).

The *red* icon indicates that an error of the type "Warning" or "PDA Error" has occurred in the system. When the red icon is in the *blinking* state, it is not a warning but indicates an error of the type "Critical Error". Detailed information on these error types is provided at the start of this list. The *gray* icon indicates that all system components are operating without error.

System Asset Tag:

Displays the System Asset Tag assigned to the system unit if applied.

Controller Time

This field specifies the blade server's current date and time.

Input Power System Limits:

This field is a link to the *Information / Operation → Operation → Power Management → Input Power Limit* page in the navigation tree. It indicates the limits configured.

For details, please refer to [section “Input Power Limit Tab” on page 59](#).

Power Consumption Mode:

This field is a link to the *Information / Operation → Operation → Power Management → Consumption* page in the navigation tree. It indicates the Consumption Modes configured.

For details, please refer to [section “Consumption Tab” on page 61](#).



This icon is optional and is displayed only if a USB stick is connected to the Master Management Blade.



You use the Locate button to switch the blade server's and management blade's ID LED *on* (blue) or *off* (gray).



The bar chart shows significant power consumption values. The text below the chart provides information about the secondary output power of the PSUs which is still available for devices in the system unit.

For details, please refer to [section “Power Consumption Display” on page 54](#).



The *gray bar at the bottom of the status frame* normally only contains the name of the component selected on the right. However, if you have selected a server blade, this bar (plus the line below it) contains additional information elements just for this blade (see figure):

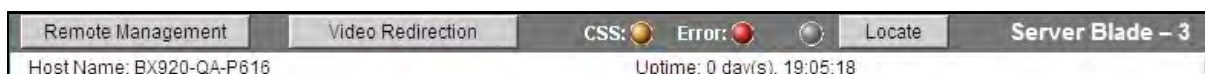


Figure 31: Additional status frame for a selected server blade

The *Remote Management* button takes you to a website where you can administer the blade remotely. You use the *Video Redirection* button to open a virtual console for the blade.

The other fields have the same meaning as described above for the status frame.

3. Navigation frame (3)

The navigation frame consists of three different views:

– Front View

Displays the BX900 S1 system unit with the existing blades (server blades and storage blades). When you point the cursor to a blade, a tooltip with the relevant name is displayed. The individual blades are clickable, i.e. after they have been clicked on, the associated information is displayed in the main frame.

i When the power supply is switched off (via *Information / Operation* → *Power Management* → *Power Switch* → *Actual System Power Status*), no blades are displayed, i.e. the unit is totally black. This power-off status is also indicated by the LED at the bottom right glowing orange instead of green.

– Rear View

Displays the BX900 S1 components at the rear (connection blades, management blades, power supply units and fan units). When you point the cursor to a component, a tooltip with the relevant name is displayed (see the picture below). The individual components are clickable, i.e. after they have been clicked on, the associated information is displayed in the main frame.



Figure 32: Front and rear views of a fully-equipped BX900 S1 system unit with tooltip information

– Tree View

The tree view contains various menu items which can be used to influence the system properties and the configuration. The individual items are clickable, i.e. after they have been clicked on, the associated information is displayed in the main frame.

i Hardware components which are not integrated into the BX900 S1 system unit are not displayed in the navigation frame, either.

Each of the three views of the navigation tree is collapsible (☐ or ☐☐).

4. Main frame (4)

The main frame supplies information about the BX900 S1 system unit. It contains information about the option/component which was selected via one of the two views or the navigation menu.

The individual server blade status is displayed in the *Server Blade Status* section using the same icons as for the overall status of the blade server system, but two additional icons are used:



The icon on the left (amber) indicates that the server blade is operating in firmware flash phase or maintenance phase.



In this phase other functions triggered by the MMB can not be executed and should not be selected by the user to avoid problems.

The icon on the right (blue) indicates that the server blade is operating in inventory boot phase or initial boot phase.

Both icons are accompanied by extended *Status* information, e. g. *Polling*, *Examine*, *Check*, *Executing*, *Running*, *Processing*, *Flash in Progress*.

5. Bottom frame (5)

The bottom frame only contains a copyright notice at the bottom left.

Error handling

Errors and warnings are displayed simultaneously in the status frame, the navigation frame and the main frame. The example below shows a start page with the complete error display in all three frames:

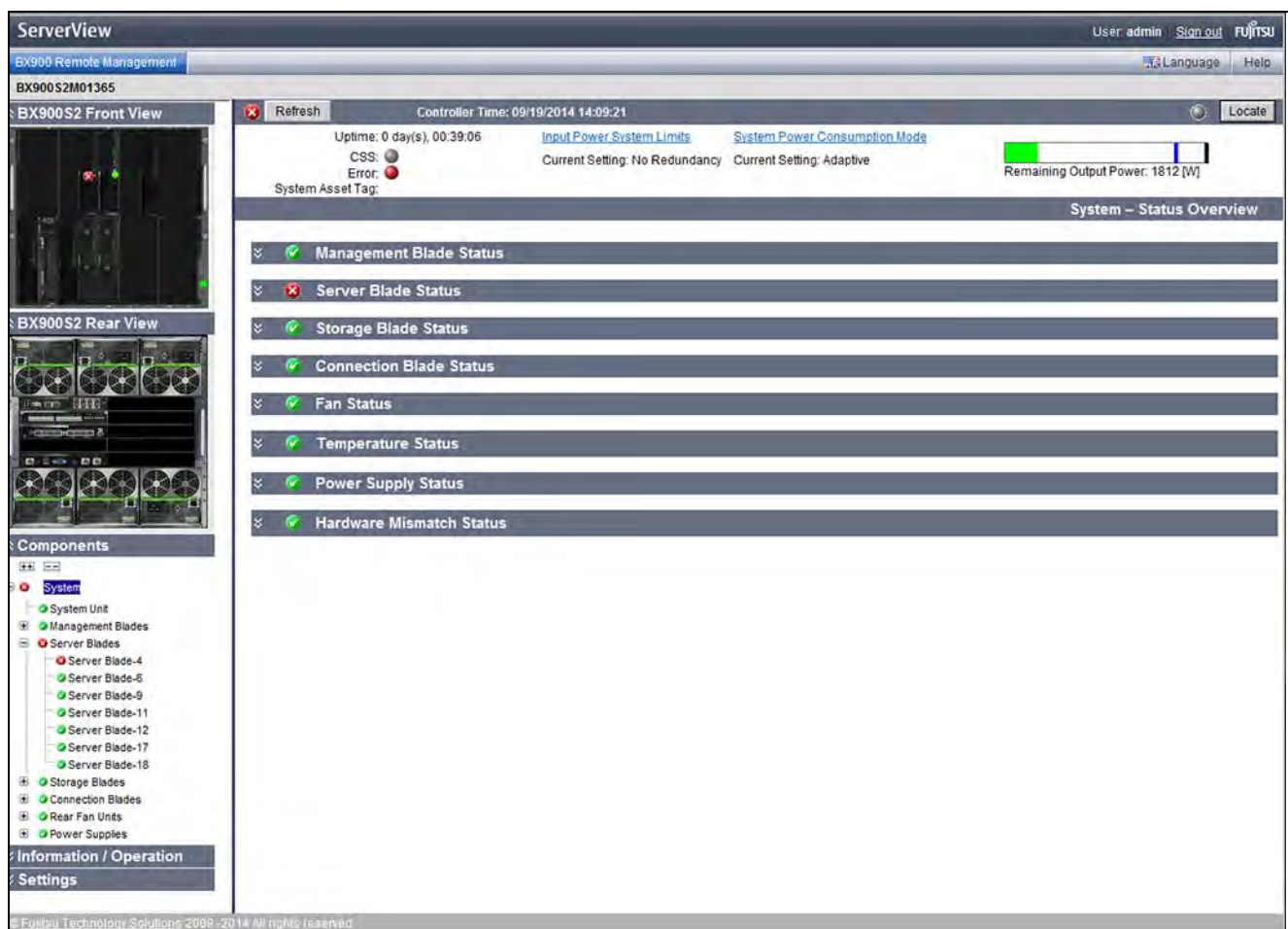


Figure 33: Start page with error display

The meaning of the error icons in the status frame has already been explained above. The  icon, which is a general indicator in the status frame for an error in the system, also appears both in the navigation frame (more precisely in the Front View and in the navigation tree) and in the main frame. This enables you to see precisely in which component the error has occurred.

The faulty Server Blade in our example is displayed a total of 6 times: 3 times in the status frame (top left and as CSS error), twice in the navigation frame (in the Front View and in the navigation tree), and in the main menu. In other words, in each case the same error is indicated.

The redundant error display on the start page has the advantage that an error is displayed even when all collapsible frames have been collapsed (see next figure):

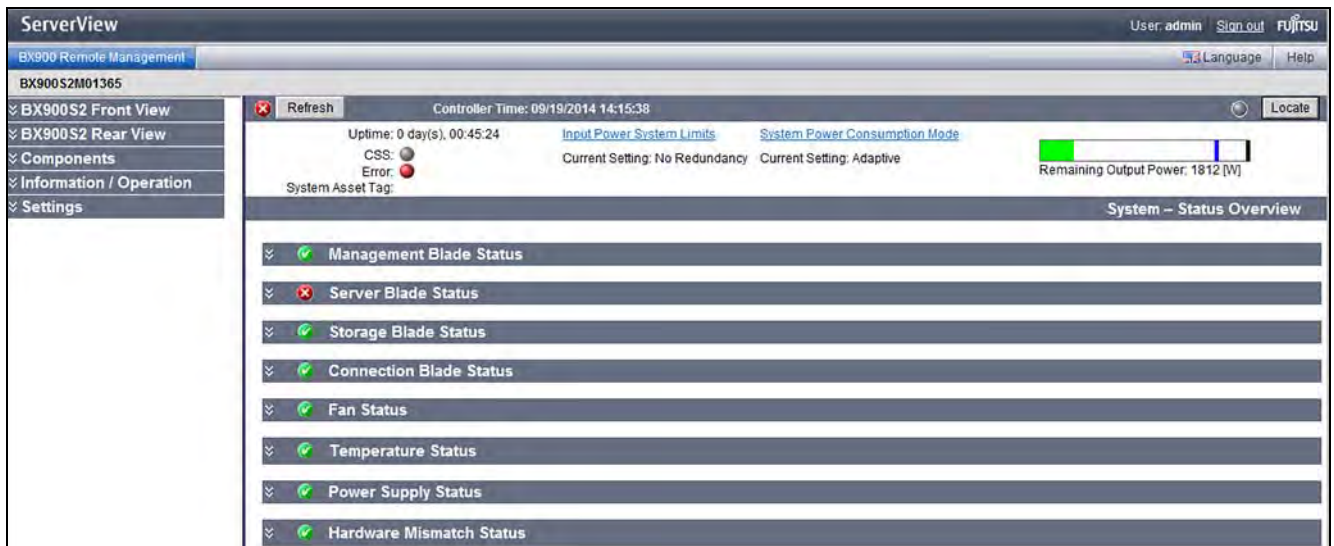


Figure 34: Start page with error display in the case of collapsed frames

i The error icon is seemingly displayed 4 times in our example (*System*, *System Unit*, *Server Blades*, *Server Blade-8* menu items) – see the next figure and detail. The reason for this is that an error is always displayed at the highest level (*System*) and is "passed down" from there.

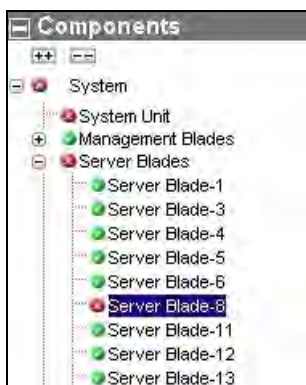


Figure 35: Error display in the navigation tree

When you point the cursor to the small  icon in the Front View, a tooltip with a corresponding message is displayed:

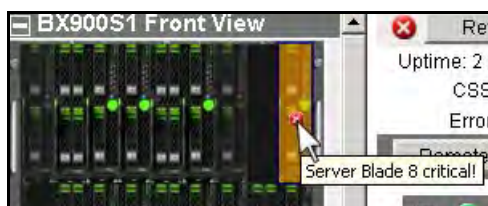


Figure 36: Error display with tooltip

4.3 Changing the User Name and Password

In the navigation frame (cf. [figure 30](#), 3) you choose the header "Information / Operation".
Open the items *Operation* → *User Management* → *Local User*.

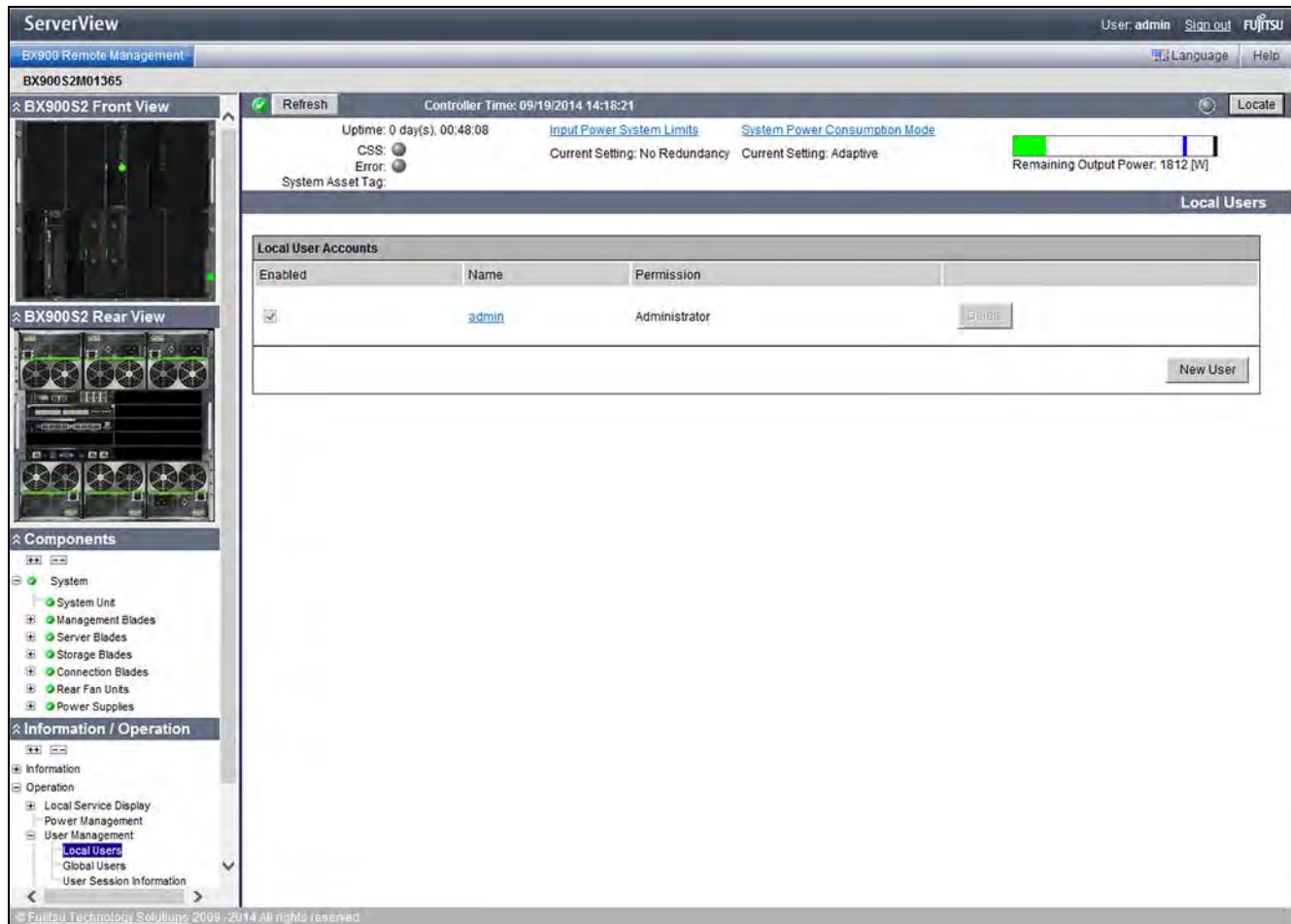


Figure 37: Choose user name

In the next screen you enter the new user name in the *Name* field and the new password in the *Password* and *Confirm Password* field:

The screenshot shows the 'ServerView' web interface for a Fujitsu BX900 Management Blade. The main window is titled 'New Local User Account'. It contains the following fields and options:

- Enabled:** ☐
- Name:**
- Password:**
- Confirm Password:**
- Permission:**
- User Shell (Text Access):**
- Special MMB Privileges:**
 - Configure System Accounts: ☐
 - Configure System Settings: ☐
- Special Server Blade Privileges:**
 - Configure User Accounts: ☐
 - Configure System Settings: ☐
 - Enable Video Redirection: ☐
 - Enable Remote Storage: ☐
- Configure Connection Blades:** ☐
- Enable User Activity Logging:** ☒
- Access Bays:**
 - Management Bays: ☐
- Server Bays:**
 - All Server Bays: ☐
 - Grid of checkboxes for Server Bays 1 through 16.
- Connection Bays:**
 - All Connection Bays: ☐
 - Grid of checkboxes for Connection Bays CB1 through CB8.

The 'Apply' button is located at the bottom right of the form.

Figure 38: Enter new user name and password

Confirm your entries with the *Apply* button.



If the administration password has been changed, the administration password of the Connection Blade needs to be changed as well. Otherwise the Management Blade couldn't acquire information from the Connection Blade.

4.4 MMB firmware upgrade via TFTP

1. Open the MMB WebUI and navigate to *Operation* → *Firmware Update*.

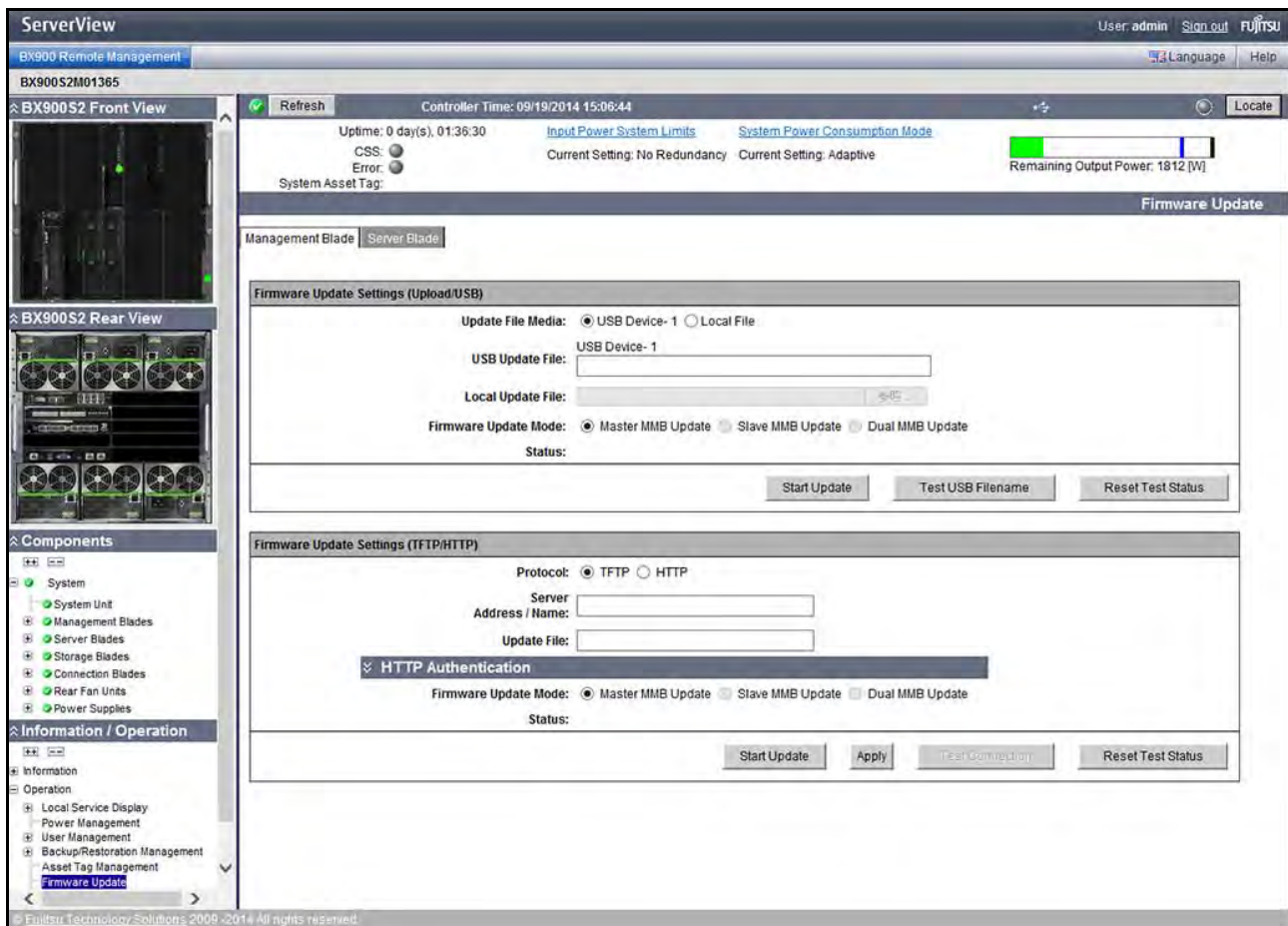


Figure 39: Firmware Update Settings (TFTP/HTTP) frame on the Firmware Update page

2. In the *Firmware Update Settings (TFTP/HTTP)* frame, select the *TFTP* radio button.
3. Specify the server in the *Server Address/Name* text field as IP address (IPv4 or IPv6) or DNS name.
4. Enter the firmware filename in the *Update File* text field as pathname.
5. Select the *Firmware Update Mode* with one of the three radio buttons:
 - *Master MMB Update* (master only)
 - *Slave MMB Update* (slave only)
 - *Dual MMB Update* (both MMBs)
6. Press the *Start Update* button.

The MMB copies the file, checks format and integrity and starts the flash procedure if no error occurred. In the case of errors the user will be informed by a status message.

After reboot of the MMB *Management Blade- $\langle n \rangle$ TFTP upgrade success* (where $\langle n \rangle = 1$ or 2) can be read as entry in the MMB event log.

4.5 MMB firmware update via USB

As an alternative to an update via *Local File* or *TFTP*, the MMB firmware can be updated via *USB Device*. For Firmware update via *HTTP* see next section.

It is possible to start the USB update via the interfaces WEB GUI and OEM SM CLP. A USB stick, formatted as FAT16, FAT32, VFAT or EXT2, with a firmware file must be used. The *Firmware Update* page got the new radio button for the *USB Device*:

1. Open the MMB WebUI and navigate to *Operation* → *Firmware Update*.
2. Insert the stick containing the firmware file into the USB socket of the MMB.

In the MMB-GUI the USB icon  appears in the grey bar at the top.

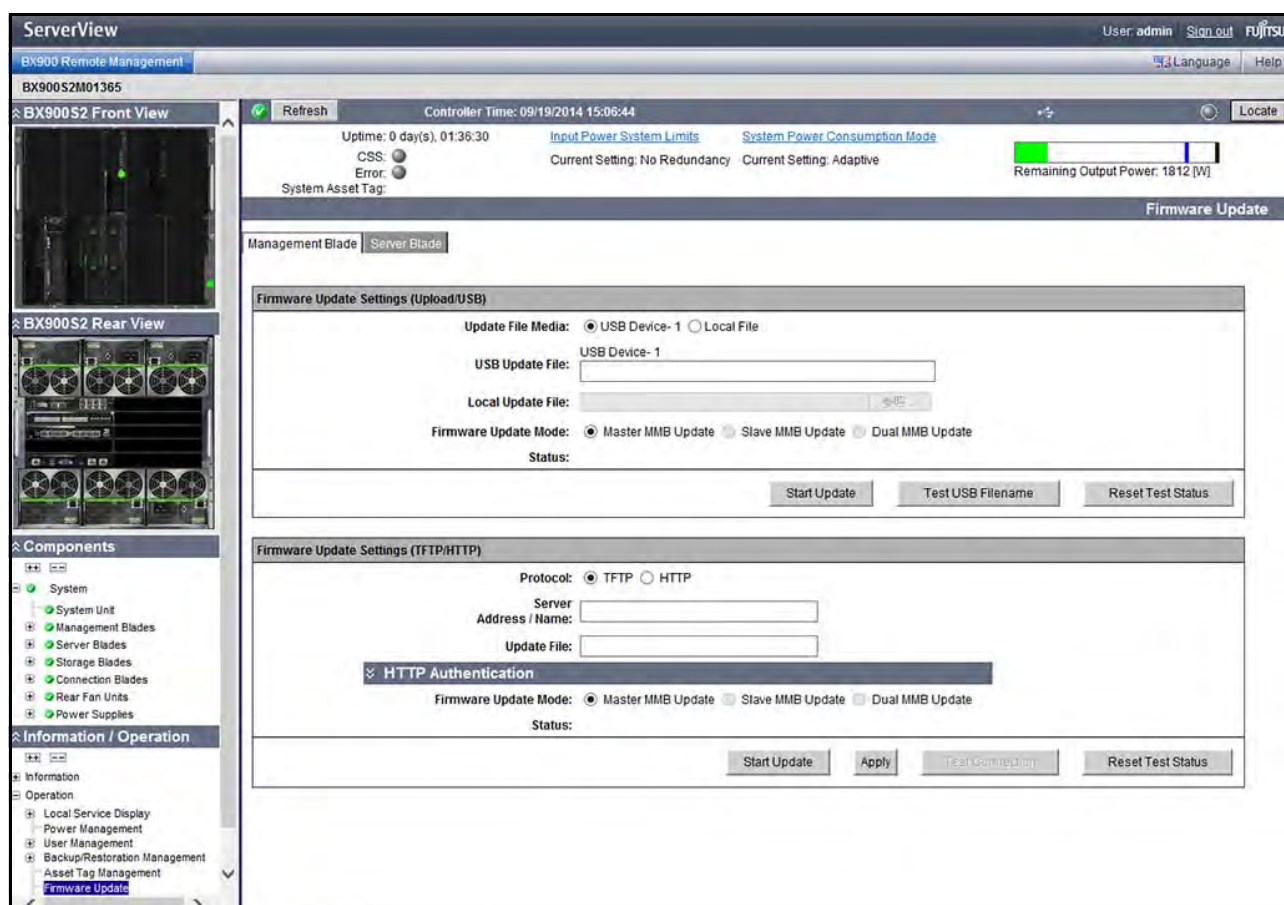


Figure 40: *Firmware Update Settings (Upload/USB)* frame on the *Firmware Update* page

3. In the *Firmware Update Settings (Upload/USB)* frame, select the *USB Device* radio button (between *Update File Media* and *Local File*).
4. Enter the firmware filename in the *USB Update File* text field. Optionally you can enter the path name separated by slash characters, not more than 255 characters.
5. Press the *Test USB Filename* button.

The MMB starts a search with the given string to localize the file and shows the result in the *Status*: line: *USB file exists* or *USB file not exists*.

6. Press the *Start Update* button.

The MMB copies the file, checks format and integrity and starts the flash procedure if no error occurred. In the case of errors the user will be informed by a status message in the same way as in the flash procedure via TFTP.

For the duration of the flash process *Do not remove USB Device from the System! Flash in Progress* is displayed.

After reboot of the MMB *Management Blade*-<n> *USB upgrade success* (where <n> = 1 or 2) can be read as entry in the MMB event log.

4.6 MMB firmware update via HTTP

The MMB firmware can also be updated via *HTTP*.

The HTTP transfer/download from a WEB server is similar to the update method via TFTP. The *Firmware Update* page got the new radio button for the *HTTP* protocol:

1. Open the MMB WebUI and navigate to *Operation* → *Firmware Update*.



Figure 41: *Firmware Update Settings (TFTP/HTTP)* frame on the *Firmware Update* page

2. In the *Firmware Update Settings (TFTP/HTTP)* frame, select the *HTTP* radio button (between *Protocol* and *HTTP*).
3. Specify the server in the *Server Address/Name* text field as IP address (IPv4 or IPv6) or DNS name.
4. Enter the firmware filename in the *Update File* text field as path name in the same way as in the flash procedure via TFTP.
5. Enter the user name in the *Server Account* text field, enter the *password* and repeat the password in the *Confirm Password* text field.
6. Press the *Test Connection* button.

The MMB shows the result in the *Status* line.

7. Select the *Firmware Update Mode* with one of the three radio buttons:
 - *Master MMB Update* (master only)
 - *Slave MMB Update* (slave only)
 - *Dual MMB Update* (both MMBs)
8. Press the *Start Update* button.

The MMB copies the file, checks format and integrity and starts the flash procedure if no error occurred. In the case of errors the user will be informed by a status message in the same way as in the flash procedure via TFTP.

After reboot of the MMB *Management Blade*-<n> *USB upgrade success* (where <n> = 1 or 2) can be read as entry in the MMB event log.

5 Power Management

The power consumption of a BX900 S1 system unit depends on the number of PSUs which are equipped in the system unit. It is important to distinguish here between the PSUs which can be seen in the Navigation Frame and the number of PSUs which are actually activated (entry *Available PSUs* under *Information / Operation* → *Operation* → *Power Management* → *Input Power Limit* → *PSU Controlling*).

The example below is based on a system unit with three activated PSUs. In addition to the PSUs three fan units are used (see figure).

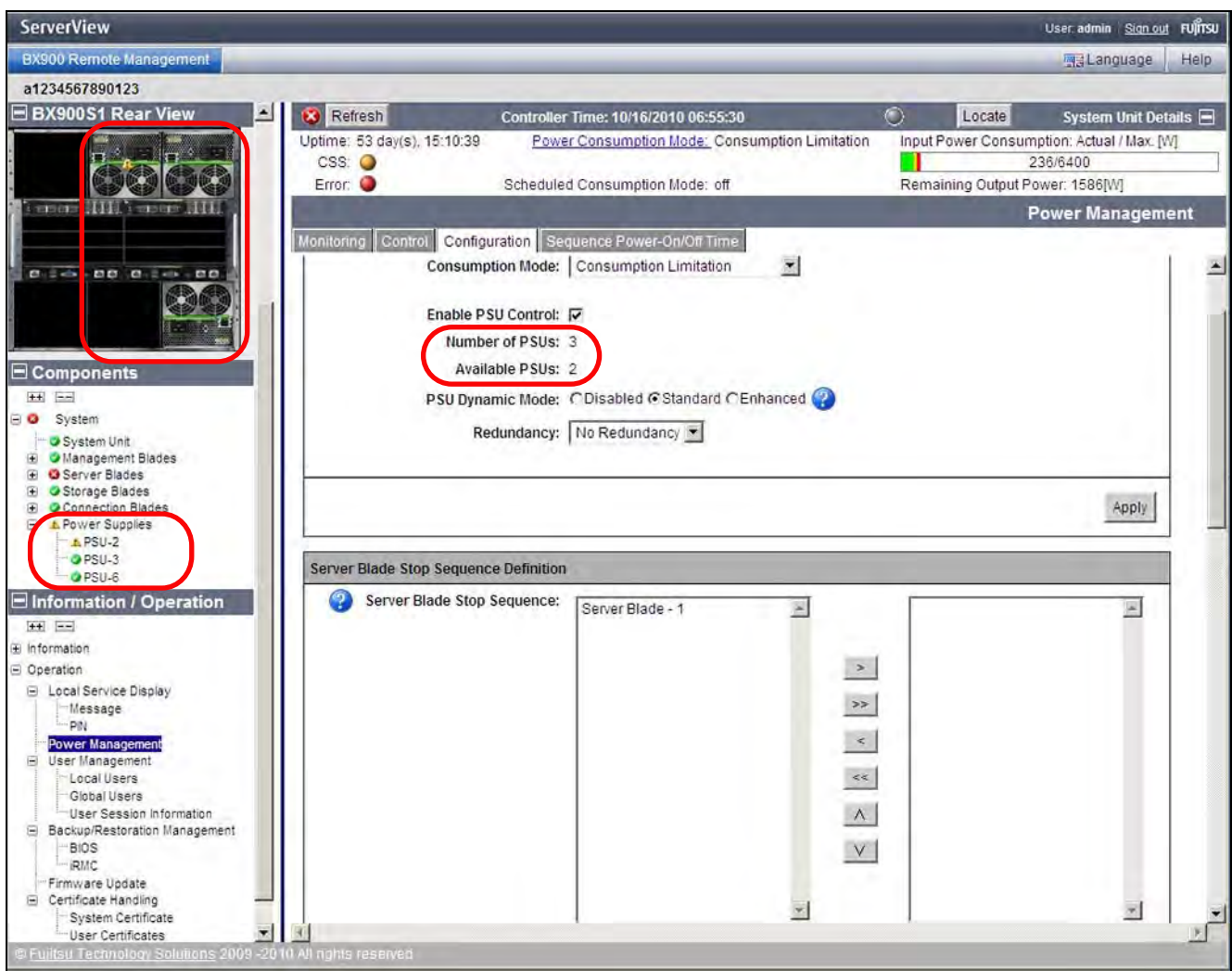


Figure 42: Display of PSUs and fan units

i Each fan unit can be substituted by an additional PSU. Each bay can be filled with a PSU or a fan unit to ensure the cooling air flow for the system unit. If a PSU fails, the number of *Available PSUs* in the *Power Consumption Options* box is decremented.

The actual power consumption of the system unit depends on the number and type of devices it is equipped with, on the current operation conditions, and on the settings which can be made on the *Information / Operation* → *Operation* → *Power Management* → *Consumption* page.

5.1 Power Consumption Display

The total power consumption is displayed at the top right in the Status Frame:

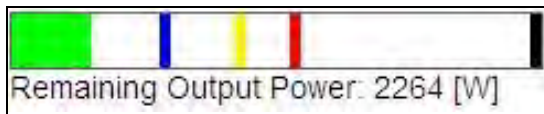


Figure 43: Display of the power consumption in the Status Frame

The bar chart shows the following power consumption values. You can display the meaning and exact value as a tooltip using the mouse:

green

Actual power consumption of the system unit from the PSU outlets (output power consumption)

blue

Maximum power budget used by the system unit from the PSU outlets

yellow

Warning threshold for the input power consumption of the PSUs

red

Configurable input power consumption limitation of the PSUs

black

Highest possible input power consumption of the PSUs

The 2nd line provides information about the secondary output power of the PSUs which is still available for devices in the system unit (without power consumption of the PSUs), depending on the PSU types and on the power management settings.

5.2 Control via Tabs

On the *Power Management* page four tabs are available which are described in detail below:

1. *History* tab
2. *Power Switch* tab
3. *Input Power Limit* tab
4. *Consumption* tab

5.2.1 History Tab

The power consumption values for the system unit are displayed on the *History* tab. Options for diagram display can be selected in the uppermost two boxes. The tab contains four boxes.

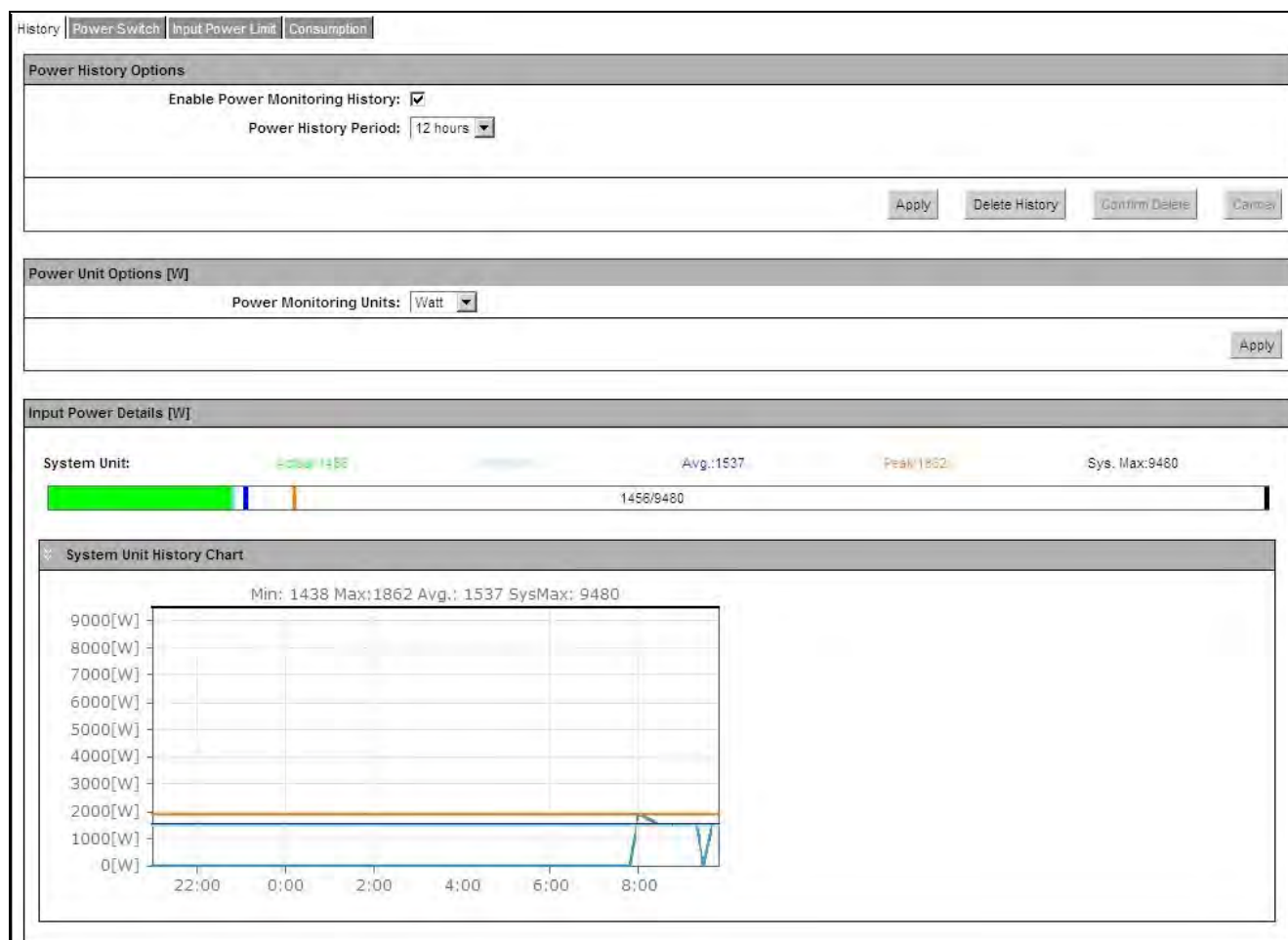


Figure 44: Power Management – *History*, display options and consumption of the system unit

Power History Options

The power consumption history can be enabled or disabled. When the history is enabled, flowcharts are displayed in addition to the bar charts.

One of seven units can be selected as the period for the flowcharts (Minimum: *1 Hour*; Maximum: *1 Year*). The period defines the period of time which is displayed in the flowcharts further below in the frame.

Power Unit Options [...]

Here you can choose between *Watt* and *BTU/h* as the unit for the power consumption values which is to be used in the diagrams.

Input Power Details [...]

A bar chart and, if enabled, a flowchart are displayed for the system unit. The various characteristic values are displayed in different colors, a key above the bar chart specifying their meaning. The following characteristic values are displayed:

- Actual power consumption
- Minimum power consumption
- Average power consumption

- Maximum power consumption
- Highest possible power consumption

5.2.2 Power Switch Tab

You can power the system unit on and off using the *Power Switch* tab. You can also power all server blades on and off provided the system unit is switched on. The tab contains six boxes.

Figure 45: Power Management – *Power Switch* tab (1/4)

Actual System Power Status

You can power off the system unit immediately (*Hard Power-off*, i.e. the system unit and all server blades are shut down at one go) or shut it down gracefully and then switch it off (*Graceful Shutdown And Off*, i.e. all server blades are shut down but the system unit remains in standby mode). You can power on the system unit if it has been switched off.

Power Switch Configuration

You can choose between *Automatic* and *Manual* for the purpose of system inventory retrieval. If *Automatic* is set, inventory retrieval takes place when server blades are added to the system unit and each time the system unit is powered on. If *Manual* is set, inventory retrieval of a server blade must, when required, be performed by powering the server blade on (see *Components* → *Server Blades* → *Power Management*).

Automatic power-off of the system unit can also be enabled when all server blades have been off for more than 30 minutes.

And for the system unit you can set power-off after the last server blade stopped.

Server Blade Power Control

If the system unit is on, you can power all server blades on and off together here. In this case the server blades are shut down gracefully and powered off or started one after the other.



Here the server blades are **not** powered on and off in the order defined in the *Server Blade Power-On/Off Sequence* box.

Scheduled System Power Switch On/Off Timer

On-Time	Off-Time	
		Sunday
08:00	17:00	Monday
08:00	17:00	Tuesday
08:00	17:00	Wednesday
08:00	17:00	Thursday
08:00	17:30	Friday
		Saturday
hh:mm	hh:mm	Every Day
Trap:	Trap:	Minutes in Advance (0-255)

Optimum Time Apply

Figure 46: Power Management – Power Switch tab (2/4)

Scheduled System Power Switch On/Off Timer

Here the power-on and power-off time for the system unit can be specified differently or identically for each weekday. To avoid conflicts with the times which have been set separately for the server blades, the *Optimum Time* button should be used to ensure that the server blade settings from the system unit setting are taken into account. Only then you should enable the settings with *Apply*.

If power consumption control was enabled under *Settings → System Unit → Alerting (Event Configuration tab, Event Log Filter box, Power Control checkbox)*, you can use the *Trap* input boxes to set the warning time at which the message is to be sent.

Server Blade Power-On/Off Sequence

Server Blade - 1
Server Blade - 2
Server Blade - 3
Server Blade - 4
Server Blade - 5
Server Blade - 6
Server Blade - 7
Server Blade - 8
Server Blade - 9
Server Blade - 10
Server Blade - 11
Server Blade - 12
Server Blade - 13
Server Blade - 14
Server Blade - 15
Server Blade - 16
Server Blade - 17
Server Blade - 18

> >> < <<

First Powered On / Last Powered Off

Last Powered On / First Powered Off

Delay Between System Power-On And First Server Blade Power-On(0-60): Minutes

Delay Between Two Server Blades Power-On/Off(0-10): Minutes

Server Blade Power-Off Action: Graceful Shutdown and Power-Off

Figure 47: Power Management – Power Switch tab (3/4)

Server Blade Power-On/Off Sequence

Here you configure the order in which the server blades are to be powered on and off. To do this, move the server blades which are to participate to the right-hand window and arrange them in descending sequence. The uppermost server blade will be powered on first and powered off last.

You can specify the time delay (in minutes) which is to exist between powering on the system unit and powering on the first server blade.

You can specify the time delay (in minutes) which is to exist between powering a server blade on/off and powering the next server blade on/off.

You can choose between *Graceful Shutdown And Power-Off* and *Hard Power-Off* when powering off the server blades.



To permit graceful shutdown of a server blade, ServerView agents must have been installed and must be active.

Slot	Type	Status	Minutes	Power Restore Policy	Force Power-Off	Delay After Power-Off Failed (1-7)	Uptime
Slot-1	BX924 S2	OK	0	Always Power Off	☐	5 Minutes	0 day(s), 02:37:03
Slot-2	BX920 S3	OK	10	Always Power Off	☐	5 Minutes	0 day(s), 02:27:02
Slot-3	BX924 S3	OK	20	Always Power Off	☐	5 Minutes	0 day(s), 02:17:02
Slot-17	BX920 S3	OK	30	Always Power Off	☐	5 Minutes	0 day(s), 02:07:00
Slot-4	Empty		5		☐	5 Minutes	
Slot-5	Empty		10		☐	5 Minutes	
Slot-6	Empty		15		☐	5 Minutes	
Slot-7	Empty		20		☐	5 Minutes	
Slot-8	Empty		25		☐	5 Minutes	
Slot-9	Empty		30		☐	5 Minutes	
Slot-10	Empty		35		☐	5 Minutes	
Slot-11	Empty		40		☐	5 Minutes	
Slot-12	Empty		45		☐	5 Minutes	
Slot-13	Empty		50		☐	5 Minutes	
Slot-14	Empty		55		☐	5 Minutes	
Slot-15	Empty		60		☐	5 Minutes	
Slot-16	Empty		65		☐	5 Minutes	
Slot-18	Empty		70		☐	5 Minutes	

Apply

Figure 48: Power Management – Power Switch tab (4/4)

In the *Power Restore Policy* column you can choose between the values *Always Power Off*, *Always Power On* and *Restore to Power State Prior to Power Loss* for each server blade which was not added to the *Server Blade Power-On/Off Sequence*.



The *Power Restore Policy* is set to *Always Power Off* for all server blades which were not added to the *Server Blade Power-On/Off Sequence* and cannot be changed.

A forced power-off can be enabled for each server blade in the fourth column in the table.

The time delay for a forced power-off after a normal power-off has failed can be set (in minutes) in the fifth column.

The table also provides information on other properties of the various server blades.

5.2.3 Input Power Limit Tab

You can use the *Input Power Limit* tab to define various settings for limiting the power consumption. The tab contains three boxes.

History | Power Switch | **Input Power Limit** | Consumption

PSU Controlling

Enable General PSU Settings: ☒

PSU Dynamic Mode: ☒ Disabled ☐ Standard ?

Redundancy:

System Power:	ON
Overall PSU Status:	OK
Present PSUs:	3
Defect PSUs:	0
Available PSUs:	3
Sleeping PSUs:	0
Working PSUs:	3
Redundancy:	No Redundancy

Apply

Input Power System Limit

Enable Input Power Limit: ☐

Currently Possible Input Power Limitation 592 - 3600: Watt ?

Apply

Input Power System Warning

Warning Threshold (1-100): Percent Of Limit Threshold

Limit Duration Time (1-7200): Seconds

Action After Limit Exceeded:

Apply

Figure 49: Power Management – *Input Power Limit* tab

PSU Controlling

Enable General PSU Settings

This checkbox must be enabled to allow you to enter the other settings in this box.

PSU Dynamic Mode

Disabled

No dynamic power supply unit mode (default).

Standard

Dynamic power supply unit mode. This setting enables power to be saved by operating some power supply units with a higher load and disabling others.



PSU Dynamic Mode together with *No Redundancy* (see the setting option below) can power off the system immediately if the last power supply unit which is still active no longer supplies sufficient power.

Redundancy

The selection options available depend on the number of power supply units available.

If power supply unit redundancy is selected ($n+1$ or $n+m$), the maximum standard output power available for the system unit is reduced, but every redundant power supply unit increases the reliability and availability of this output power level because 1 or m power supply unit(s) can fail without operations being interrupted. Two power supply units are required for the smallest redundant PSU configuration in a BX900 system unit. Possible values: *No Redundancy*, 2+1, 3+1, 4+1, 5+1, 2+2, 3+3.

On the right-hand side of the box the power on/off status and the power supply unit status of the system unit are displayed. The following terms require explanation:

Present PSUs

Total number of power supply units connected.

Defective PSUs

Number of defective power supply units.

Available PSUs

Number of operational power supply units.

Sleeping PSUs

Number of power supply units in standby mode.

Working PSUs

Number of active power supply units.

Input Power System Limit

Enable Input Power Limit

In order to specify the other settings in this box (*Input Power System Limit*) and in the *Input Power System Warning* box, this checkbox must be enabled.

Currently Possible Input Power Limitation [range]

The input power obtained by the power supply units can be limited here. The value must be contained in the predefined range.

Input Power System Warning

Warning Threshold (1 - 100)

Defines a percentage which, when reached, causes the system unit to issue a warning.

Limit Duration Time (1- 7200)

Defines the length of time (in seconds) for which the threshold status will be tolerated.

Action After Limit Exceeded

Defines which action (*Continue*, *Graceful Shutdown And Power-Off* or *Hard Power-Off*) is executed after the limit value which has been set is reached.

5.2.4 Consumption Tab

The *Consumption* tab enables the power consumption mode for the system unit to be configured and the power consumption limits for individual server blades to be defined. The tab contains five boxes.

History Power Switch Input Power Limit Consumption

System Power Consumption Modes

☒ Adaptive
☐ Minimum
☐ Server Controlled
☐ Scheduled

Apply

Adaptive Mode

Re-Evaluation Period (1-60): 15 Minutes

Re-Evaluation Policy: ☒ Consumption Demand ☐ Server Blade Priority

Apply

Server Controlled Consumption Mode Table

■ Current Consumption
 ■ Controllable Range
 ■ Avg.
 ■ Peak
 ■ Blade Max.
 ■ Limit

Select	Slot	Blade Name	Consumption Mode	Input Limit Watt	Actual / Input Max. Watt
☐	1	BX924S3-PCM	Adaptive		141/289
☐	2	BX920S3-999	Adaptive		43/131
☐	3	BX924S3235	Adaptive		87/203
☐	17	BX924S3235	Adaptive		71/227

Select All Deselect All Set for the selected Servers: Apply

Temporary Power Sample Period: 12 hours (takes effect only for Avg. and Peak) Refresh All

Figure 50: Power Management – Consumption tab (1/2)

System Power Consumption Modes

One of several power consumption modes can be defined for the system unit here.

Adaptive

Default setting. Controls the power consumption of the server blades according to one of two strategies: according to the consumption of the blades or according to their priority. Further settings for this mode can be specified in the second or fifth box on the tab.



Details of the concept of adaptive budgeting are provided in the last section [5.2.4.1 on page 63](#) of this chapter (please read up front).

Minimum

Sets power consumption to the lowest possible value.



This mode forces a CPU clock with the lowest possible speed, thus enabling the lowest power consumption to be achieved.

Server Controlled

Enables the settings which can be entered individually for the various server blades in the third box (*Server Controlled Consumption Mode Table*).

Scheduled

An alternative to the modes which can be selected above it which permanently determine the mode for the server blades. Enables the time-of-day-dependent mode settings which can be specified jointly for all server blades in the *Scheduled Server Blade Consumption* box.

Adaptive Mode

The settings in this box are enabled when *Adaptive* mode is selected in the *System Power Consumption Modes* box.

Re-Evaluation Period (1 - 60)

Specifies the re-evaluation period (in minutes) for the power consumption mode *Adaptive*.

Re-Evaluation Policy

Select *Consumption Demand*, when the power budget available for server blades is to be distributed according to their power consumption in the past. Select *Server Blade Priority*, when the power budget available for server blades is to be distributed according to their priority. The priority is determined by the *Adaptive Budgeting Priority Table* box (box at the bottom).

Server Controlled Consumption Mode Table

The settings in this box are enabled when *Controlled* mode is selected in the *System Power Consumption Modes* box.

This box is used to select the server blades individually and to leave consumption control to the iRMC of the server blade (with the mode and consumption limit specified there) or to define a consumption limit for the selected server blade.

On the right of the box the input power values for each server blade are displayed in the form of a colored bar chart. The evaluation period can be selected for the diagram values Avg. and Peak (Minimum: 1 Hour; Maximum: 1 Year).

History | Power Switch | Input Power Limit | Consumption

Consumption Schedule For All Server Blades

Time 1	Mode 1	Time 2	Mode 2	
	Adaptive		Adaptive	Sunday
	Adaptive		Adaptive	Monday
	Adaptive		Adaptive	Tuesday
	Adaptive		Adaptive	Wednesday
	Adaptive		Adaptive	Thursday
	Adaptive		Adaptive	Friday
	Adaptive		Adaptive	Saturday

HH:MM Adaptive HH:MM Adaptive Every Day

Adaptive Budgeting Priority Table

- Server Blade - 18
- Server Blade - 17
- Server Blade - 16
- Server Blade - 15
- Server Blade - 14
- Server Blade - 13
- Server Blade - 12
- Server Blade - 11
- Server Blade - 10
- Server Blade - 9
- Server Blade - 8
- Server Blade - 7
- Server Blade - 6
- Server Blade - 5
- Server Blade - 4
- Server Blade - 3
- Server Blade - 2
- Server Blade - 1

Apply

Figure 51: Power Management – Consumption tab (2/2)

Consumption Schedule For All Server Blades

The settings in this box are enabled when *Scheduled* mode is selected in the *System Power Consumption Modes* box.

Here two different or identical times, each of which is assigned to a consumption mode, can be specified for the system unit and for each weekday.

Adaptive Budgeting Priority Table

This priority table enables the server blades to be arranged in order to specify a sequence of priorities. The server blade at the top has the highest priority.

The priority table of the server blades is evaluated in various cases:

- In the consumption mode *Adaptive, Server Blade Priority* strategy, the table controls the assignment of the consumption budget.
- If consumption limitation is configured for the system unit, the table controls which server blades are off or are not switched on when power-on takes place.
- In the event of excessive power consumption as the result of a fault, the table controls the emergency shutdown sequence of the server blades. The shutdown starts with the server blade at the bottom of the table which has the lowest priority.

5.2.4.1 Concept of Adaptive Budgeting

Adaptive budgeting enables more server blades to be operated in a BX900 chassis than would be permitted with a standard power budget. In addition to the fixed chassis components, the maximum power consumption of the individual server blades is normally added in order to calculate the power budget. The maximum power consumption of an individual server blade varies depending on the blade configuration. This ensures that the entire system also has adequate reserves, even when operating under full load.

If the system no longer has any power budget available, no additional server blades can be switched on, although individual servers frequently do not use their maximum budget.

Adaptive budgeting bypasses this problem by re-calculating the budget for the individual server blades at specific time intervals. Two strategies can be used to calculate the budget in an "adaptive" way. The adaptive budget is generally calculated on the basis of the average consumption of late. To do this, the power consumption of the last evaluation period is used as a basis and periodically re-adapted.

Alternatively, the server priority table can also be used as a policy.

Two different options are available for the periodic re-calculation of the budget. One option is to measure the consumption of the individual blades for the period defined and to then use this with a safety reserve as a new power budget for this server. The other option is to prioritize the blades. The blade with the highest priority receives the most from the power budget. The priority is defined in the *Adaptive Budgeting Priority Table*. The blade at the top has the highest priority.

Adaptive budgeting can be activated within the *Consumption* tab, first box *System Power Consumption Modes*. It is set by default.

6 Global User Management

Global MMB user management using roles

Global MMB user management via an LDAP directory server requires no extension to the standard directory server schema. Instead, all the information that is relevant for the MMB is provided via additional LDAP groups and organizational units (OUs) which are combined in separate OUs in a domain of the LDAP directory server. This additional groups can be imported with the SVS_LdapDeployer.

Users obtain fixed privileges according their Authorization Roles declared in the organizational unit (OU) SVS.

There are three interfaces to Global User Management:

1. Active Directory (for Windows systems)
2. OpenLDAP (for Linux systems)
3. eDirectory (for Windows and Linux systems)

6.1 Configuring an Active Directory Server

6.1.1 Installing the Windows Active Directory Server

First a Windows Server Operation System (Microsoft Windows Server 2003, 2008 or 2008 R2, in this example Windows Server 2008 R2) is installed on any server.

After this has been installed, the following roles must be installed and configured:

- Active Directory (AD) Domain Services
- DNS Server (may be installed during execution of DCPROMO, if necessary)
- DHCP Server (optional)

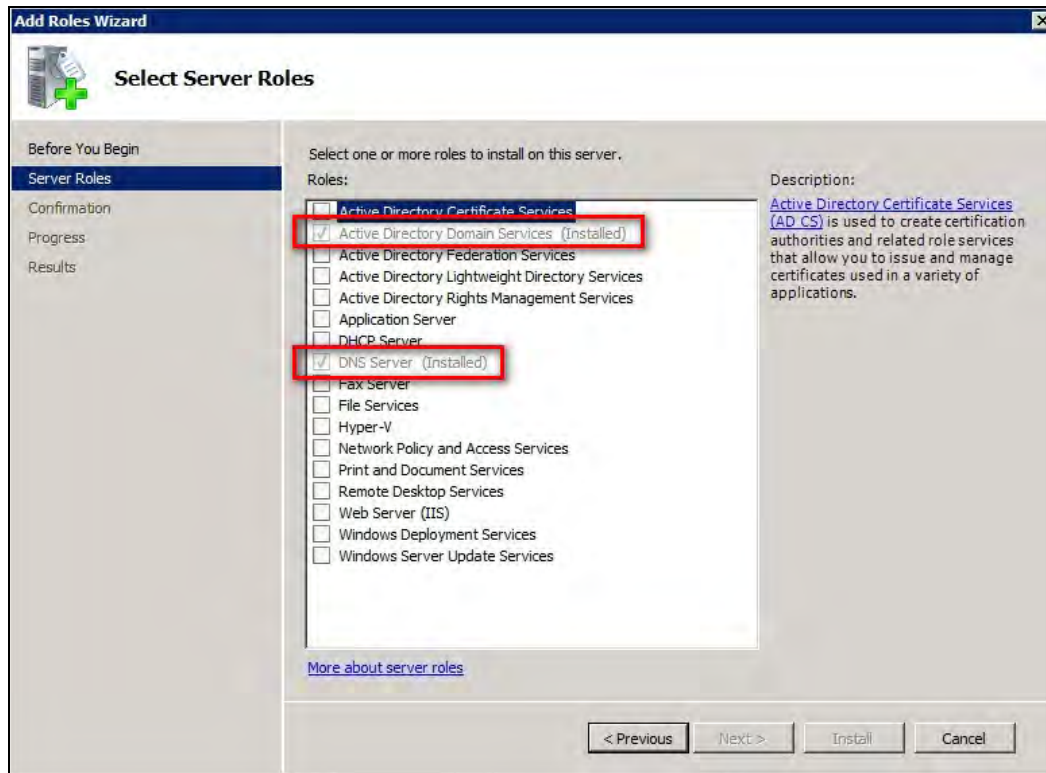


Figure 52: AD – server roles

6.1.2 Creating the LDAP Structure (based on Microsoft Active Directory)

To permit the management blade to be accessed by means of an LDAP user, a particular structure consisting of Organizational Units (OUs) and Groups must be set up. A sample configuration is described here.

The tool *SVS_LDAPDeployer* (v. 1.00.09209) can be used to create the structure. The tool can be used from any system with network access to the Active Directory Server on which at least JAVA v1.5 is installed.

The configuration file *Generic_InitialDeploy.xml* is included in the *SVS_LDAPDeployer* software package and should be edited according to your specific needs before deploying the structure in the Active Directory.

The following sections should be edited:

- <DirectoryService> : Contains the IP and Port of the Active Directory Server.
- <DirectoryType> : Sets the type of LDAP directory, in this example *Microsoft AD*.
- <root> : Contains the root level of your domain, e.g. for testdomain1.local "*dc=testdomain1,dc=local*".
- <username> : Contains the administrator's user name in the notation *username@domain.org*, e.g. *Administrator@testdomain1.local*.
- <Department name> : The name of the department where the structure will be created, e.g. *TestDepartment*.
- If the password section is left blank, the *SVS_LDAPDeployer* will ask for the administrator's password during execution.

When configuration is finished you can execute the *SVS_LDAPDeployer* by opening a CMD window, navigating to the *SVS_LDAPDeployer* directory and issuing the following command:

```
# java -jar SVS_LdapDeployer.jar -deploy Configuration_InitialDeploy_Generic.xml
```

The *SVS_LDAPDeployer* starts, asks for the administrator's password and creates the structure in the Active Directory which is needed to authenticate users of the MMB.

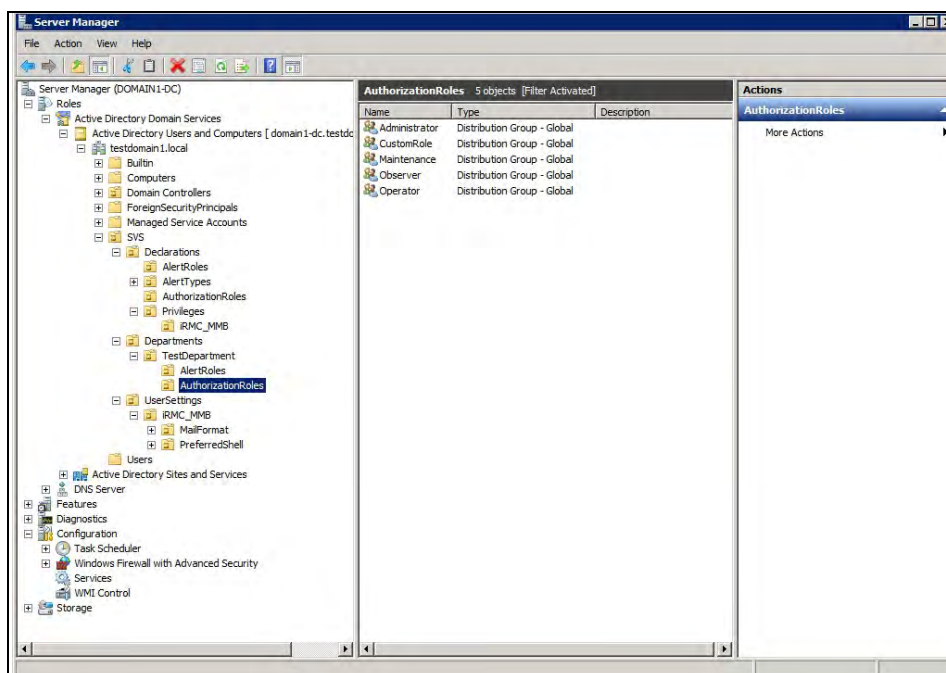


Figure 53: Active Directory: SVS

6.1.3 Assigning Domain Users to the MMB

To enable a user to log in on the management blade as a domain user, *AuthorizationRoles* must be set for this user:

1. Create a new user if none exists.
2. Navigate to *SVS* → *Departments* → *[YourDepartment]* → *AuthorizationRoles*
3. Open the properties of the desired role and add the user as a member in the **Members** tab.
(Multiple selection is permitted for a user.)

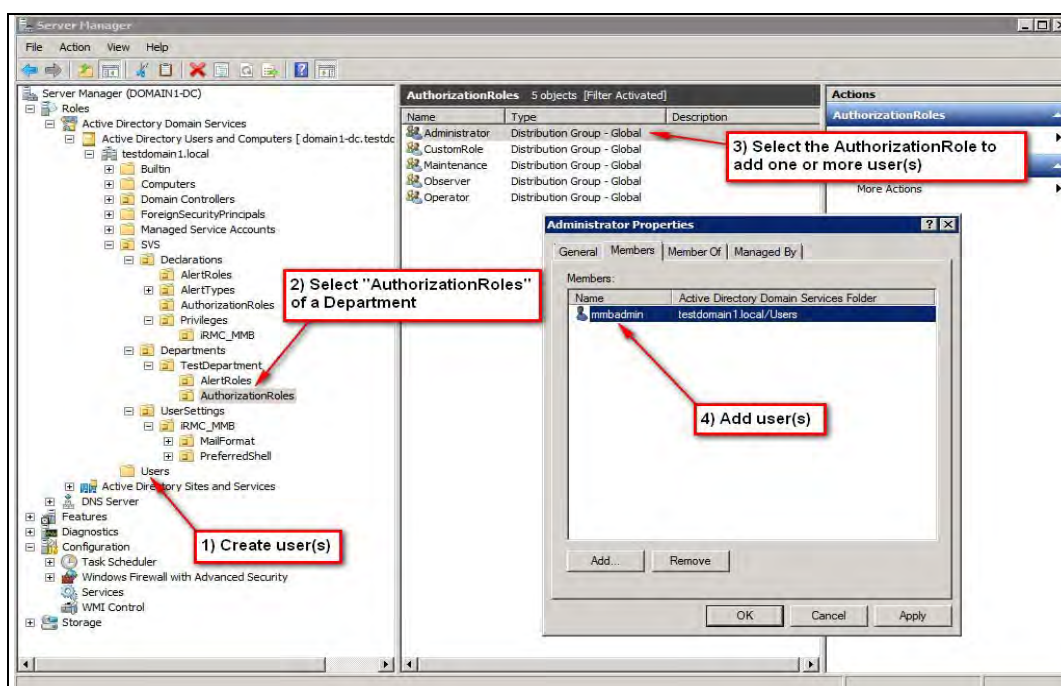


Figure 54: Active Directory: Users

6.1.4 Setting up the Management Blade

Open the BX900 MMB WebUI in advanced mode and navigate to *Information/Operation* → *User Management* → *Global Users*. The following screenshot shows an example of the settings required for communication with a Windows Active Directory:

1. Enable LDAP: Enables LDAP authentication.
2. Enable LDAP SSL: Enables SSL communication between the MMB and the Active Directory Server. (The MMB does not need a certificate and does not check the certificate delivered by the LDAP server.)
3. Disable Local Login: Disables the option of logging in without LDAP authentication.
4. Always Use SSL Login: Enables only SSL logins at the MMB WebUI. (This option will be enabled automatically, LDAP requires HTTPS to be enabled.)
5. Directory Server Type: Sets the LDAP Server type. (Windows Active Directory).
6. LDAP Server: IP address of the LDAP Server.
7. Domain Name: Name of the domain. (e.g. *testdomain1.local*).
8. Base DN: Assigned automatically.
9. Groups Directory As Sub-Tree From Base DN: Not required.
10. Dept. Name: Name of the department.
11. LDAP Auth. User Name: Not required.
12. LDAP Auth. User Password: Not required.

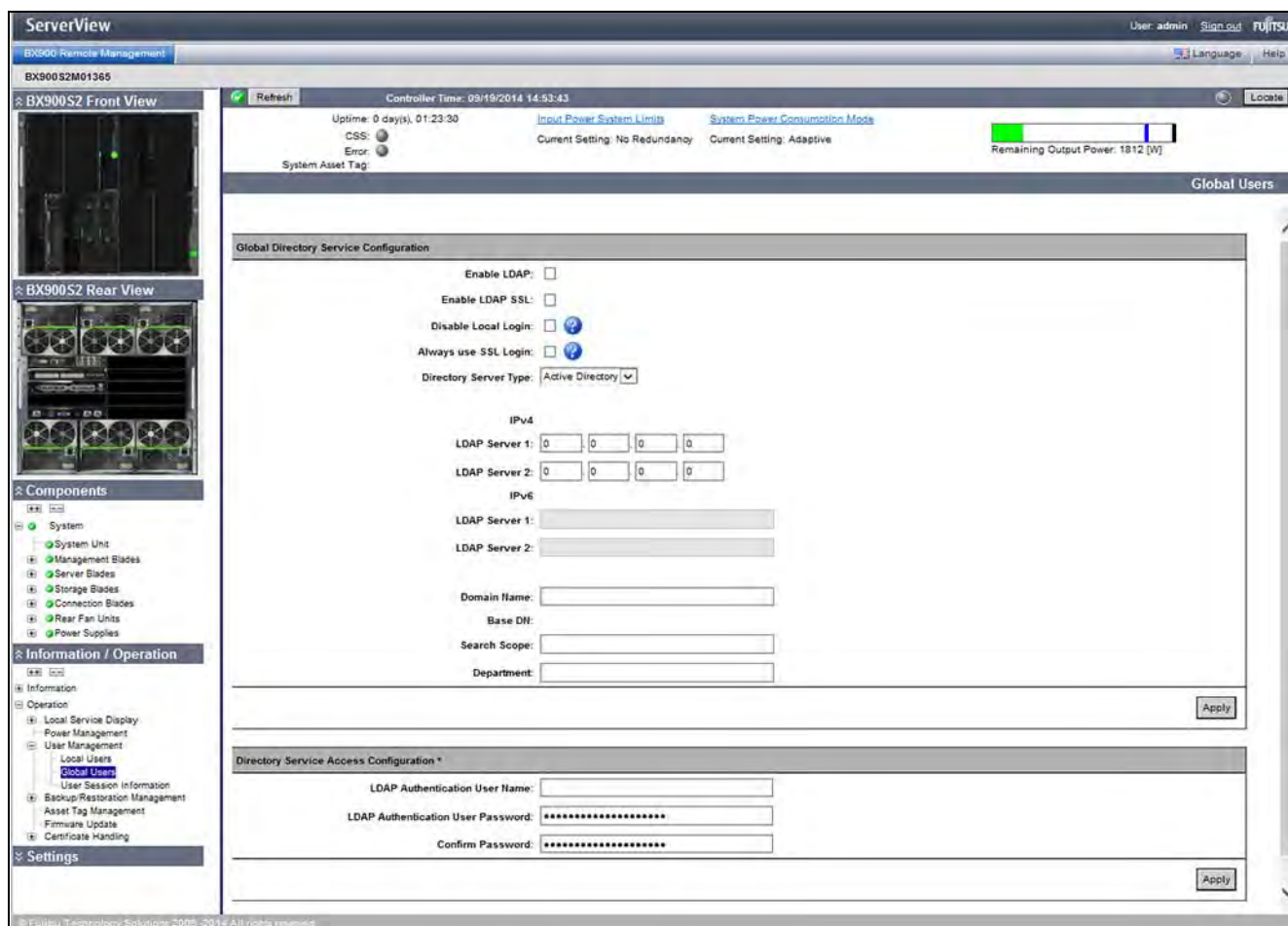


Figure 55: MMB settings Web User Interface

Alternatively MMB configuration can be performed using the SMASH-CLP interface.

Open the BX900 MMB SMASH-CLP interface and navigate to the target:
/OemFujitsuSiemens/AgentInfo/LdapAuthentication.

The settings are the same as in the WebUI and can be set using the command notation:
set [property]="[value]", e.g. **set AgentLdapRootDomainName="testdomain1.local"**
 A *Help* command is available for every writeable property, e.g. *help AgentLdapType*.

```

COM1 - PuTTY
</OemFujitsuSiemens/AgentInfo/LdapAuthentication> BX900S1 -> show
status = 0
status_tag = COMMAND COMPLETED

/OemFujitsuSiemens/AgentInfo/LdapAuthentication
Properties
  AgentLdapAuthenticationEnable = disable
  AgentLdapType = Windows Active Directory
  AgentLdapOverSsl = disable
  AgentLdapServerIp1 = 172.17.176.3
  AgentLdapServerIp2 = 0.0.0.0
  AgentLdapServerIpv61 =
  AgentLdapServerIpv62 =
  AgentLdapRootDomainName = testdomain1.local
  AgentLdapBaseDn = dc=testdomain1,dc=local
  AgentLdapUserBaseDn =
  AgentLdapUserBaseDepartment = TestDepartment
  AgentLdapSpecialUserAccount =
  AgentLdapSpecialUserPassword = *****
Verbs
  cd show

</OemFujitsuSiemens/AgentInfo/LdapAuthentication> BX900S1 ->
  
```

Figure 56: MMB settings SMCLP

6.1.5 Logging in on the Management Blade as an AD User

When a user logs in on the management blade as an AD user, the domain is appended in the login mask. The notation is [username]@[domain] (e.g. [mmbadmin@testdomain1.local](#)).



Figure 57: Active Directory: Login WebUser Interface

Whether the login was correct can be checked on the web interface.

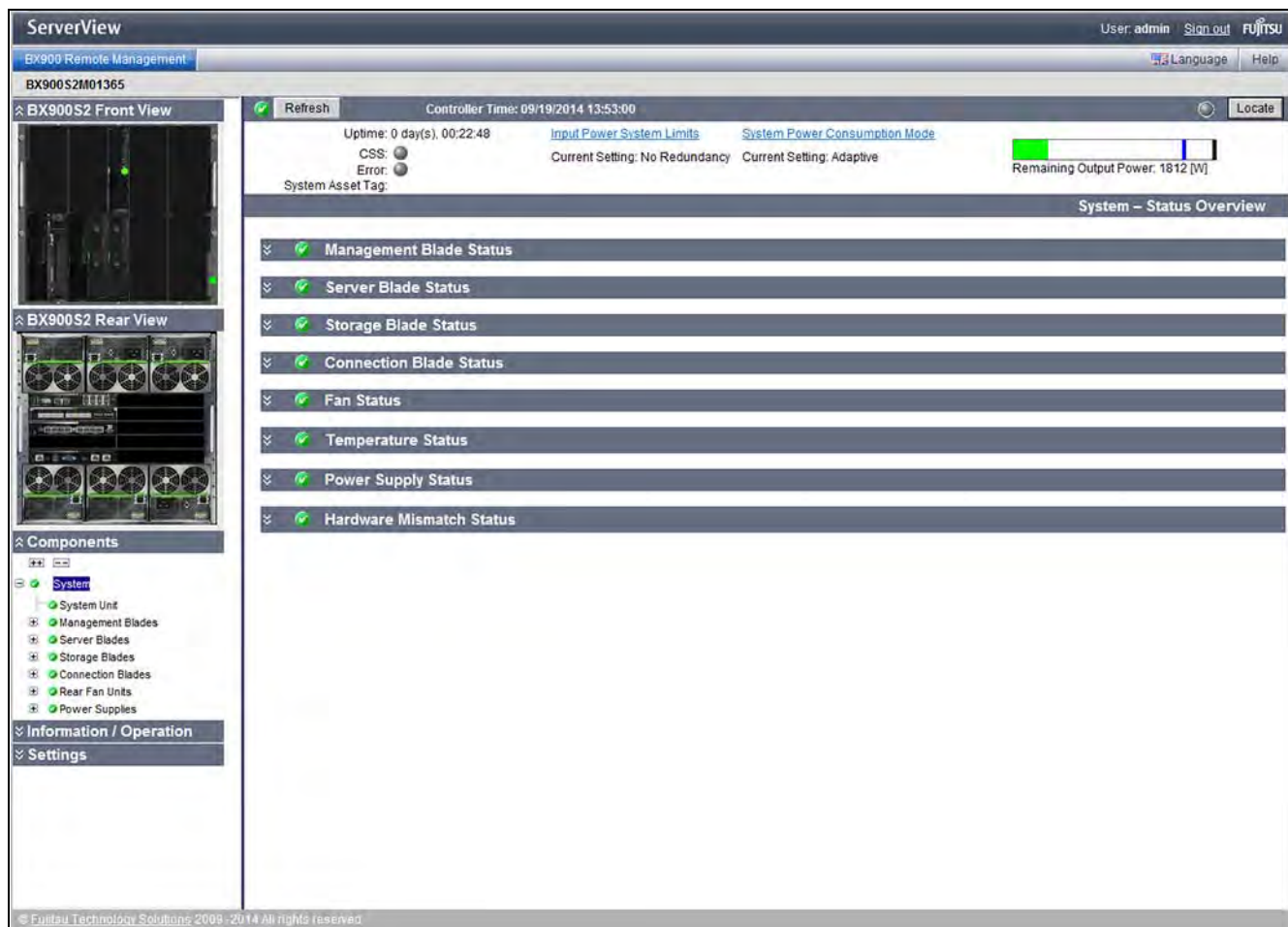


Figure 58: Check Login

6.2 Configuring an openLDAP Server

6.2.1 Base Configuration of openLDAP

A RedHat Enterprise Linux Server is taken as a basis. The services required were selected during system installation (openLDAP Server packages).

Set up openLDAP as a system service.

After installation is complete the configuration files are located at */etc/openldap*.

Open the file *slapd.conf* and edit the following entries to create the base structure of the domain:

```
database bdb
suffix "dc=<MY-DOMAIN>,dc=<COM>"
rootdn "cn=Manager,dc=<MY-DOMAIN>,dc=<COM>"
rootpw secret
directory /usr/local/var/openldap-data
```

For example edit the lines to:

```
database bdb
suffix "dc=testdomain2,dc=local"
rootdn "cn=Manager,dc=testdomain2,dc=local"
rootpw testen
directory /usr/local/var/openldap-data
```

To apply the changes just restart LDAP using the command:

```
# service ldap restart
```

In order to connect to the domain it is necessary to set up a base structure. This is done by using the *ldapadd* command and an *ldif* configuration file. Because there is no sample configuration file in */etc/openldap/* you must create one from scratch.

Create a new file named *<my-name>.ldif*, e.g. in this example *testdomain2.ldif*, open it with an editor of your choice and create the following content:

```
dn: dc=<MY-DOMAIN>,dc=<COM>
objectclass: dcObject
objectclass: organization
o: <EXAMPLE ORGANISATION>
dc: <MY-DOMAIN>

dn: cn=<ACCOUNTNAME>,dc=<MY-DOMAIN>,dc=<COM>
objectclass: organizationalRole
cn: <ACCOUNTNAME>
```

Or as in the example:

```
dn: dc=testdomain2,dc=local
objectclass: dcObject
objectclass: organization
o: TestOrganization
dc: testdomain2

dn: cn=Manager,dc=testdomain2,dc=local
objectclass: organizationalRole
cn: Manager
```

The first part will create the base domain structure and the second part an administrator account.

After the file is saved the structure can be created by *ldapadd* using the following command:

```
# ldapadd -x -D "cn=<ACCOUNTNAME>,dc=<MY-DOMAIN>,dc=<COM>" -W -f example.ldif
```

Or as in the example:

```
# ldapadd -x -D "cn=Manager,dc=testdomain2,dc=local" -W -f testdomain2.ldif
```

After the base structure is created various LDAP browsers can be used to view and manage the domain (e.g. *phpLDAPadmin*).

6.2.2 Creating the LDAP Structure (Based on openLDAP)

To permit the management blade to be accessed by means of an LDAP user, a particular structure consisting of Organizational Units (OUs) and Groups must be set up. A sample configuration is described here.

The tool *SVS_LDAPDeployer* (v. 1.00.09209) can be used to create the structure. The tool can be used from any system with network access to the openLDAP Server which has at least Java v1.5 installed.

The configuration file *Generic_InitialDeploy.xml* is included in the *SVS_LDAPDeployer* software package and should be edited according to your specific needs before deploying the structure into the openLDAP directory.

The following sections should be edited:

- *<DirectoryService>* : Contains the IP and Port of the openLDAP Server.
- *<DirectoryType>* : Sets the type of LDAP directory, in this example *Open LDAP*.
- *<root>* : Contains the root level of your domain, e.g. for *testdomain2.local* "*dc=testdomain2,dc=local*".
- *<username>*: Contains the manager's user name in the notation "*cn=Manager,dc=testdomain2,dc=local*".

- <Department name> : The name of the department where the structure will be created, e.g. *TestDepartment*.
- If the password section is left blank, *SVS_LDAPDeployer* will ask for the administrator's password during execution.

When the configuration is finished you can execute the *SVS_LDAPDeployer* by opening a CMD window, navigating to the *SVS_LDAPDeployer* folder and using the following command:

```
# java -jar SVS_LdapDeployer.jar -deploy Configuration_InitialDeploy_Generic.xml
```

The *SVS_LDAPDeployer* starts, asks for the manager's password and creates the structure in the *Open LDAP* directory which is needed to authenticate users of the MMB.

6.2.3 Assigning Domain Users to the MMB

To enable a user to log in on the management blade as a domain user, *AuthorizationRoles* must be set for this user:

1. Create a new user if none exists.
2. Navigate to *SVS* → *Departments* → [*YourDepartment*] → *AuthorizationRoles*.
3. Add the user to the desired role as a member and make sure you set the *UID* to match the login name.

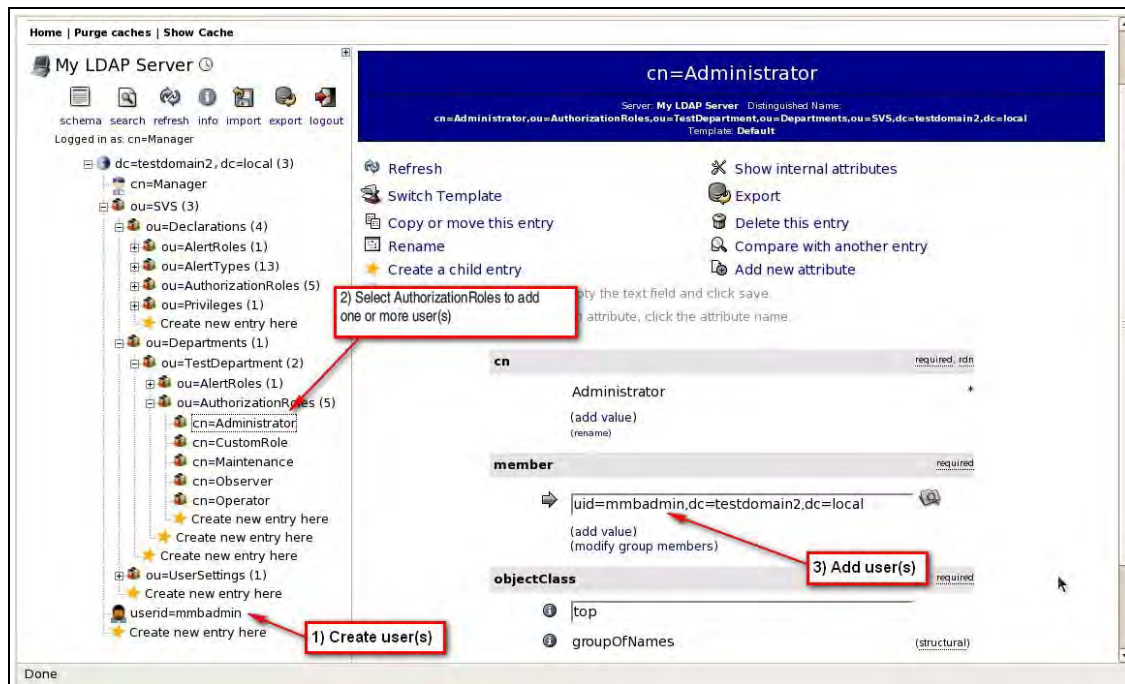


Figure 59: Domain Users for MMB

6.2.4 Setting up the Management Blade

Open the BX900 MMB WebUI in advanced mode and navigate to *Information/Operation* → *User Management* → *Global Users*. The following screenshot shows an example of the settings required for communication with an openLDAP Server:

1. Enable LDAP: Enables LDAP authentication.
2. Enable LDAP SSL: Enables SSL communication between the MMB and the openLDAP Server.
(The MMB does not need a certificate and does not check the certificate delivered by the LDAP server.)
3. Disable Local Login: Disables the option of logging in without LDAP authentication.

4. Always Use SSL Login: Enables only SSL logins at the MMB WebUI. (This option will be enabled automatically, LDAP requires HTTPS to be enabled.)
5. Directory Server Type: Sets the LDAP Server type (*OpenLDAP*).
6. LDAP Server: IP address of the LDAP Server.
7. Domain Name: Name of the domain (e.g. *testdomain2.local*).
8. Base DN: Assigned automatically.
9. Groups Directory As Sub-Tree From Base DN: Not required.
10. Dept. Name: Name of the department.
11. LDAP Auth. User Name: Management account of the openLDAP Server in the notation "cn=Manager,dc=testdomain2,dc=local".
12. LDAP Auth. User Password: Password of the manager account.

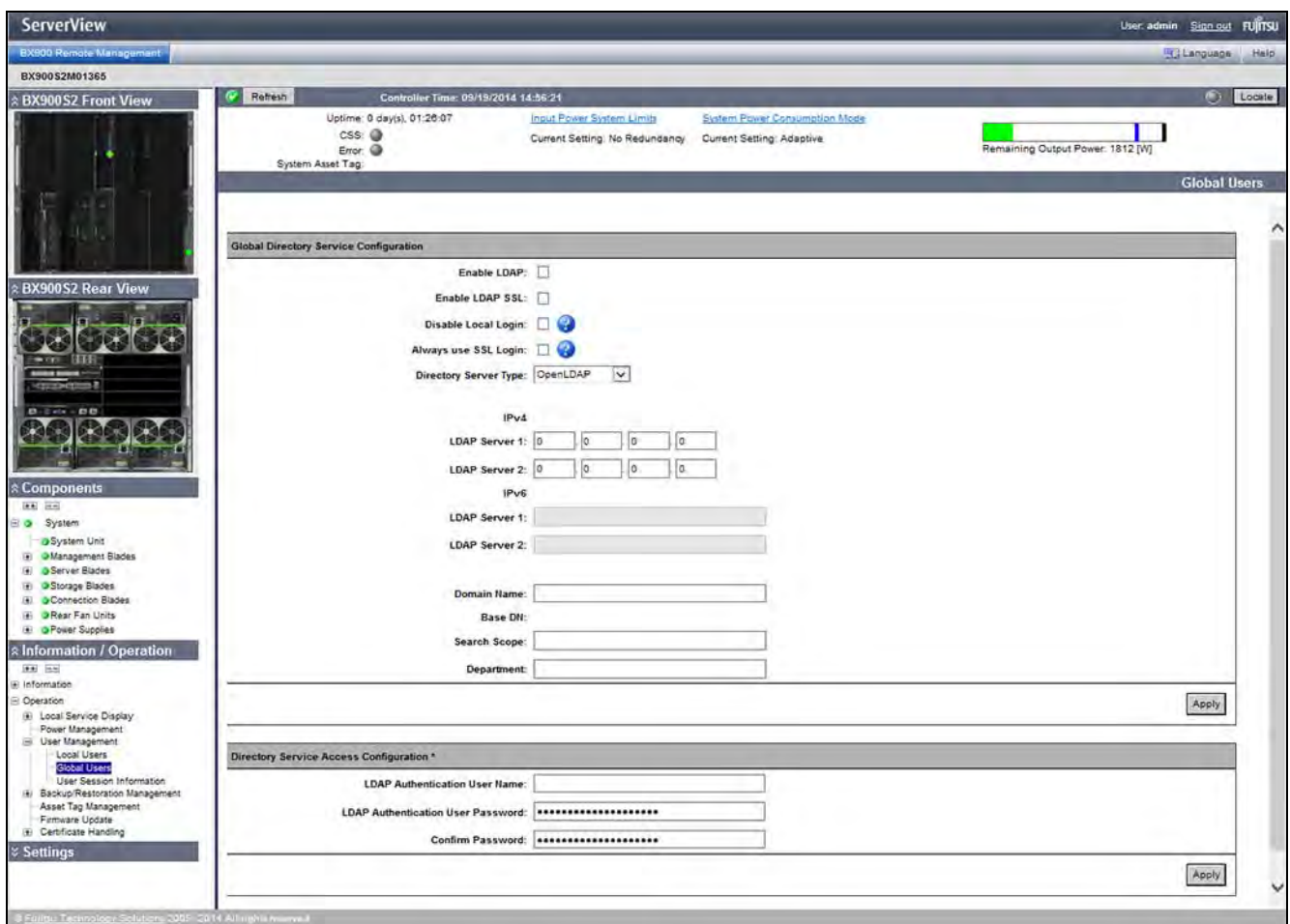


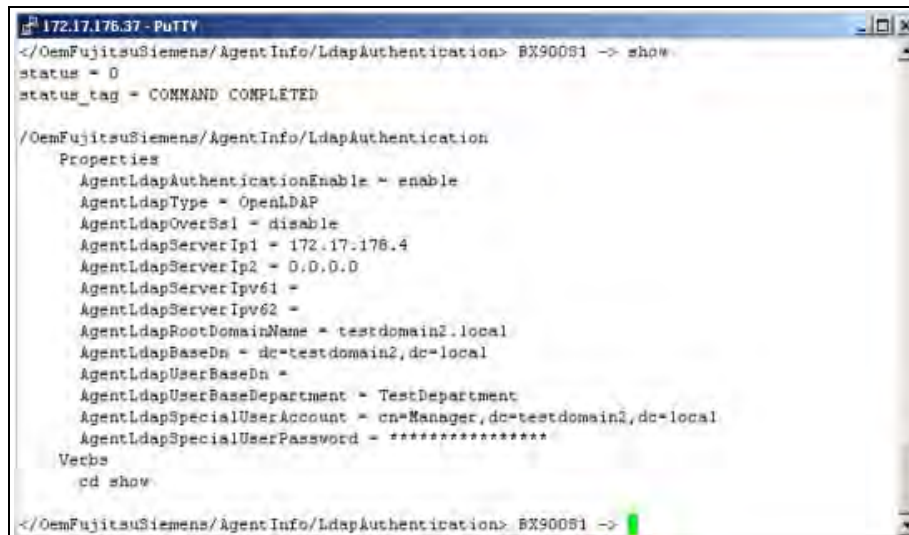
Figure 60: LDAP settings on the management blade

Alternatively MMB configuration can be performed using the SMASH-CLP interface.

Open the BX900 MMB SMASH-CLP interface and navigate to the target *OemFujitsuSiemens/AgentInfo/LdapAuthentication*.

The settings are the same as in the WebUI and can be set using the command notation: `set [property]=[value]`, e.g. `set AgentLdapRootDomainName="testdomain2.local"`

A *Help* command is available for every writeable property, e.g. `help AgentLdapType`.



```
172.17.176.37 - PuTTY
</OemFujitsuSiemens/AgentInfo/LdapAuthentication> BX900S1 -> show
status = 0
status_tag = COMMAND COMPLETED

/OemFujitsuSiemens/AgentInfo/LdapAuthentication
Properties
  AgentLdapAuthenticationEnable = enable
  AgentLdapType = OpenLDAP
  AgentLdapOverSsl = disable
  AgentLdapServerIp1 = 172.17.176.4
  AgentLdapServerIp2 = 0.0.0.0
  AgentLdapServerIpv61 =
  AgentLdapServerIpv62 =
  AgentLdapRootDomainName = testdomain2.local
  AgentLdapBaseDn = dc=testdomain2,dc=local
  AgentLdapUserBaseDn =
  AgentLdapUserBaseDepartment = TestDepartment
  AgentLdapSpecialUserAccount = cn=Manager,dc=testdomain2,dc=local
  AgentLdapSpecialUserPassword = *****
Verbs
  cd show

</OemFujitsuSiemens/AgentInfo/LdapAuthentication> BX900S1 ->
```

Figure 61: LDAP settings using SMASH-CLP interface

6.2.5 Logging in on the Management Blade as an openLDAP User

No special notation is needed to log in to the MMB as an openLDAP user. The login name and password can be used as configured in the LDAP Server.



Figure 62: Logging in on the management blade as an LDAP user

Whether the login was correct can be checked on the web interface.

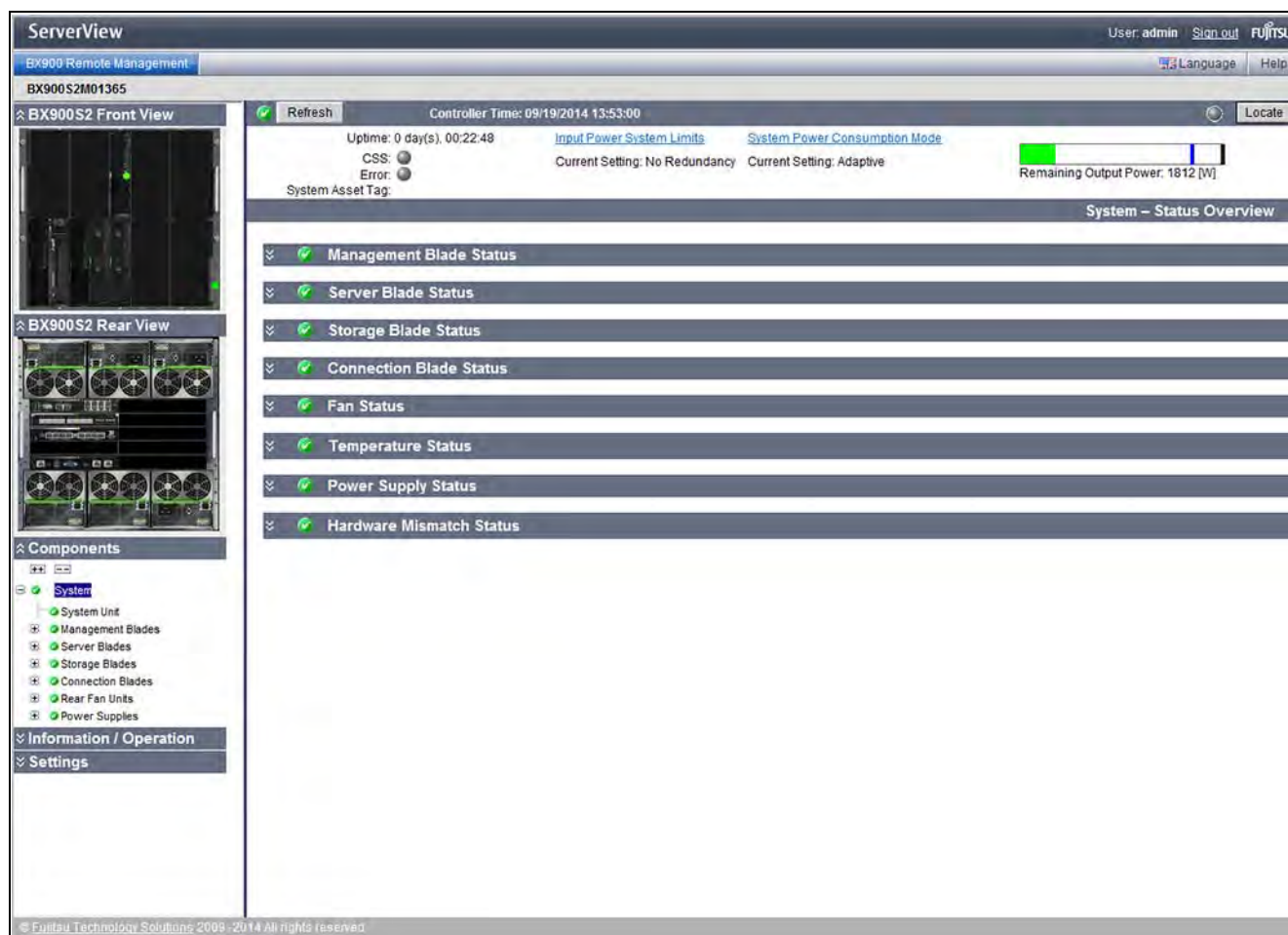


Figure 63: Correct login on the web user interface

6.3 Configuring an eDirectory Server

6.3.1 Installing the eDirectory Server

Novell eDirectory is available for many operating systems. In this manual a Windows Server 2008 R2 system is used as the basis for eDirectory installation. The Novell iManager is used to administer the eDirectory after installation. (When using iManager with Internet Explorer 8 make sure you set the browser to *Compatibility Mode*.)

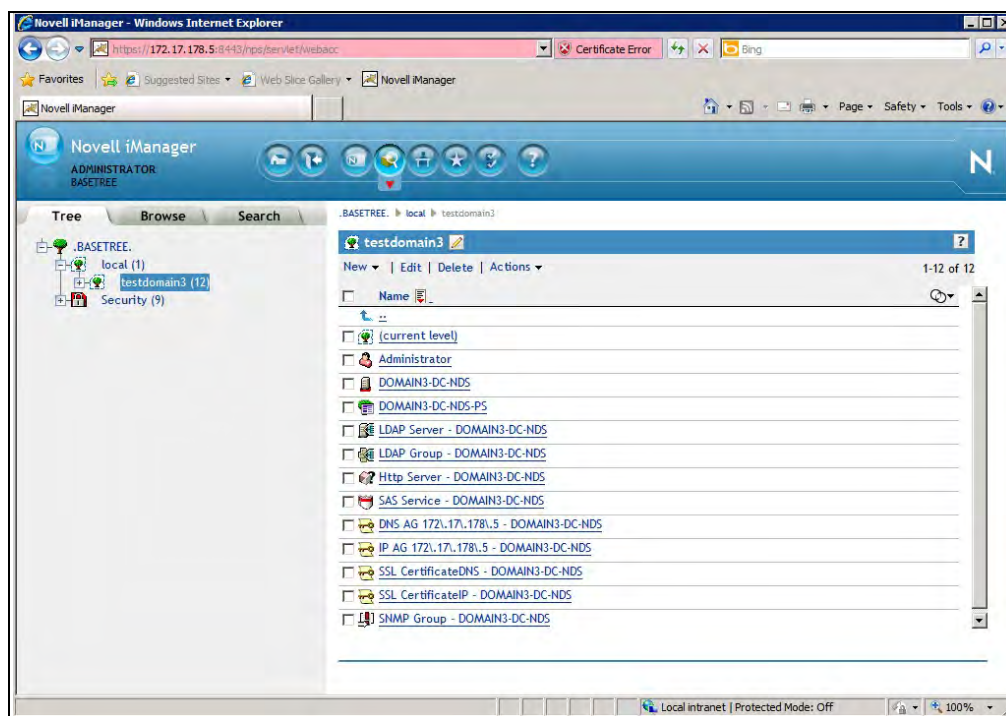


Figure 64: eDirectory installation

6.3.2 Creating the LDAP Structure (Based on eDirectory)

To permit the management blade to be accessed by means of an LDAP user, a particular structure consisting of Organizational Units (OUs) and Groups must be set up. A sample configuration is described here.

The tool *SVS_LDAPDeployer* (v. 1.00.09209) can be used to create the structure. The tool can be used from any system with network access to the eDirectory Server which has at least Java v1.5 installed.

The configuration file *Generic_InitialDeploy.xml* is included in the *SVS_LDAPDeployer* software package and should be edited according to your specific needs before deploying the structure in the eDirectory.

The following sections should be edited:

- <DirectoryService> : Contains the IP and Port of the eDirectory Server.
- <DirectoryType> : Sets the type of LDAP directory, in this example *eDirectory*.
- <root> : Contains the root level of your domain, e.g. for testdomain3.local "`dc=testdomain3,dc=local`".
- <username>: Contains the Administrator's user name in the notation "`cn=Administrator,dc=testdomain3,dc=local`".
- <Department name> : The name of the department where the structure will be created, e.g. *TestDepartment*.
- If the password section is left blank, *SVS_LDAPDeployer* will ask for the administrator's password during execution.

When configuration is performed you can execute the *SVS_LDAPDeployer* by opening a CMD window, navigating to the *SVS_LDAPDeployer* folder and using the following command:

```
# java -jar SVS_LdapDeployer.jar -deploy Configuration_InitialDeploy_Generic.xml
```

The *SVS_LDAPDeployer* starts, asks for the administrator's password and creates the structure in the eDirectory which is needed to authenticate users of the MMB.

6.3.3 Assigning Domain Users to the MMB

To enable a user to log in on the management blade as a domain user, *AuthorizationRoles* must be set for this user:

1. Create a new user if none exists.
2. Navigate to *SVS* → *Departments* → *[YourDepartment]* → *AuthorizationRoles*.
3. To add the user to the desired role as a member, mark the role and select *Edit*. In the popup window add the user to the **Members** tab.

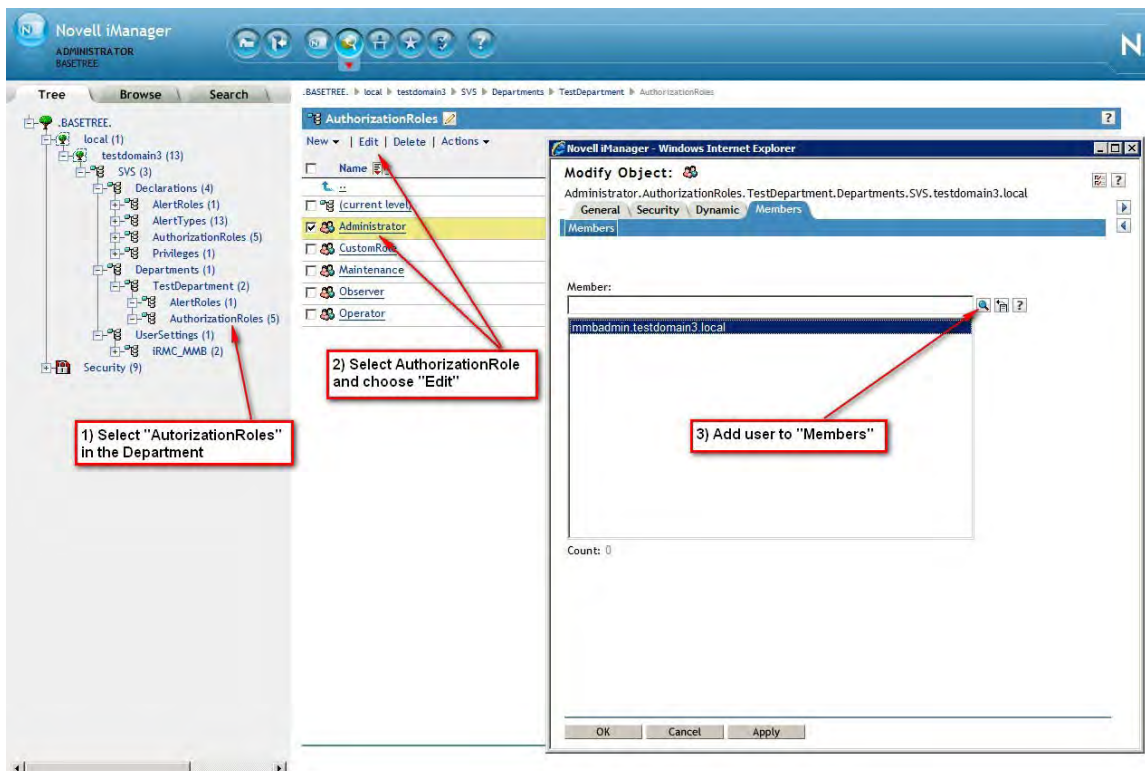


Figure 65: eDirectory SVS user

6.3.4 Setting up the Management Blade

Open the BX900 MMB WebUI in advanced mode and navigate to *Information/Operation* → *User Management* → *Global Users*. The following screenshot shows an example of the settings required for communication with an eDirectory Server:

1. Enable LDAP: Enables LDAP authentication.
2. Enable LDAP SSL: Enables SSL communication between the MMB and the eDirectory Server. (The MMB does not need a certificate and does not check the certificate delivered by the LDAP server.)
3. Disable Local Login: Disables the option of logging in without LDAP authentication.
4. Always Use SSL Login: Enables only SSL logins at the MMB WebUI. (This option will be enabled automatically, LDAP requires HTTPS to be enabled.)
5. Directory Server Type: Sets the LDAP Server type (*eDirectory*).
6. LDAP Server: IP address of the LDAP Server.
7. Domain Name: Name of the domain (e.g. *testdomain3.local*).
8. Base DN: Assigned automatically.
9. Groups Directory As Sub-Tree From Base DN: Not required.
10. Dept. Name: Name of the department.
11. LDAP Auth. User Name: Management account of the eDirectory Server in the notation "*cn=Manager,dc=testdomain3,dc=local*".
12. LDAP Auth. User Password: Password of the manager account.

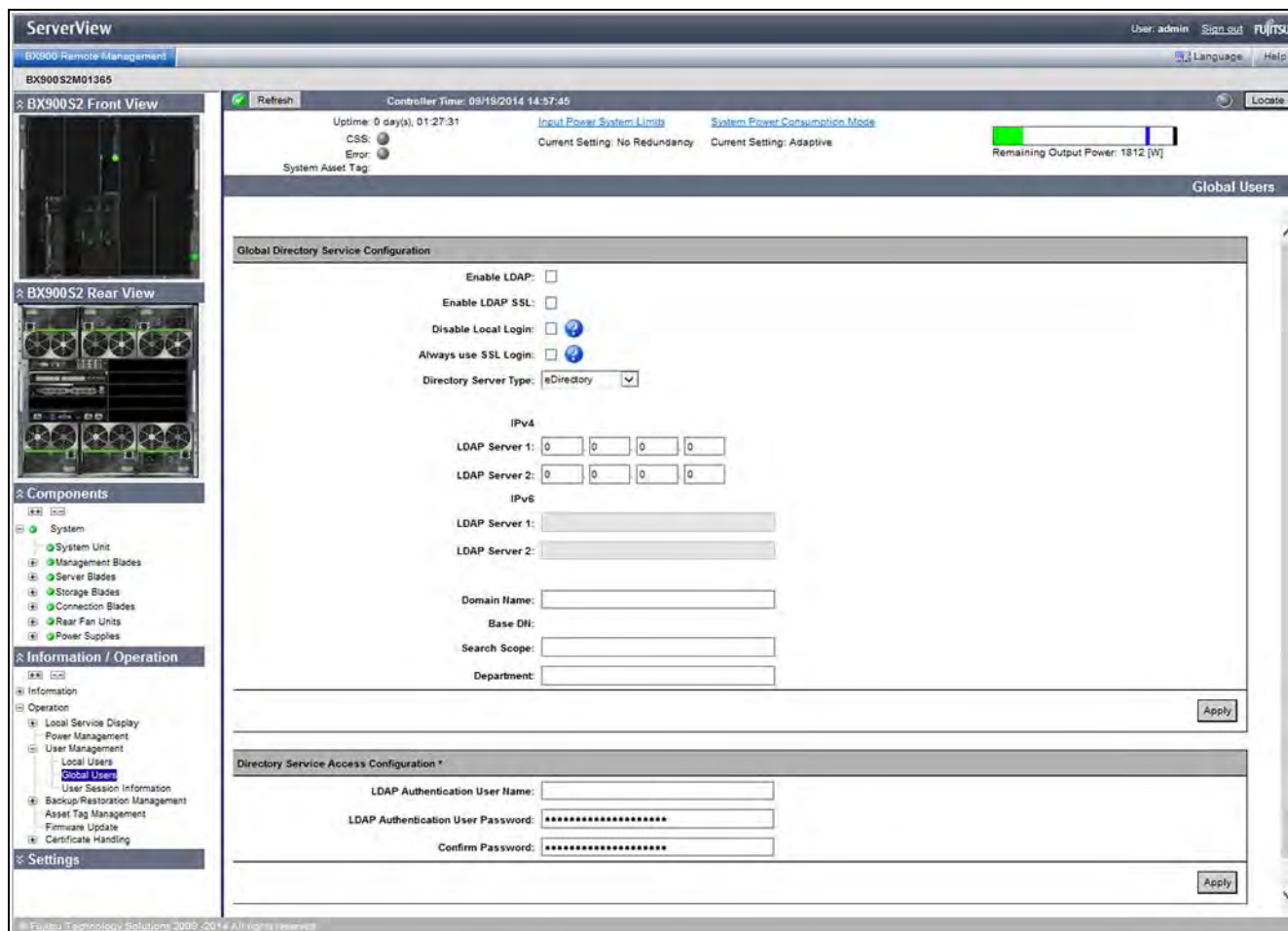


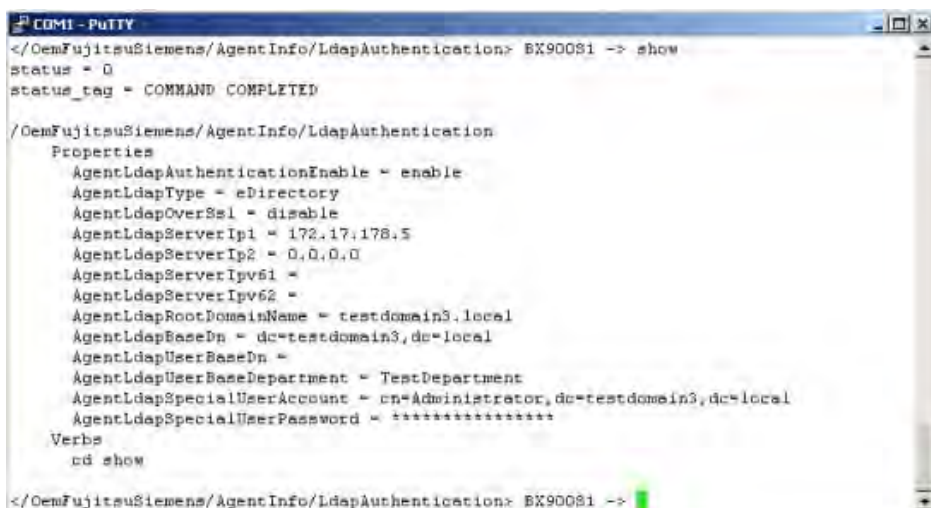
Figure 66: eDirectory MMB settings web user interface

Alternatively the MMB configuration can be performed using the SMASH-CLP interface.

Open the BX900 MMB SMASH-CLP interface and navigate to the target `/OemFujitsuSiemens/AgentInfo/LdapAuthentication`.

The settings are the same as in the WebUI and can be set using the command notation: `set [property]="[value]"`, e.g. `set AgentLdapRootDomainName="testdomain3.local"`

A `Help` command is available for every writeable property, e.g. `help AgentLdapType`.



```
COM1 - PuTTY
</OemFujitsuSiemens/AgentInfo/LdapAuthentication> BX900S1 -> show
status = 0
status_tag = COMMAND COMPLETED

/OemFujitsuSiemens/AgentInfo/LdapAuthentication
Properties
  AgentLdapAuthenticationEnable = enable
  AgentLdapType = eDirectory
  AgentLdapOverSsl = disable
  AgentLdapServerIp1 = 172.17.178.5
  AgentLdapServerIp2 = 0.0.0.0
  AgentLdapServerIpv61 =
  AgentLdapServerIpv62 =
  AgentLdapRootDomainName = testdomain3.local
  AgentLdapBaseDn = dc=testdomain3,dc=local
  AgentLdapUserBaseDn =
  AgentLdapUserBaseDepartment = TestDepartment
  AgentLdapSpecialUserAccount = cn=Administrator,dc=testdomain3,dc=local
  AgentLdapSpecialUserPassword = *****
Verbs
  cd show

</OemFujitsuSiemens/AgentInfo/LdapAuthentication> BX900S1 ->
```

Figure 67: eDirectory MMB settings SMCLP

6.3.5 Logging in on the Management Blade as an eDirectory User

No special notation is needed when logging in to the MMB as an eDirectory user. The login name and password can be used as configured in the LDAP Server.



Figure 68: eDirectory login on web user interface

Whether the login was correct can be checked on the web interface.

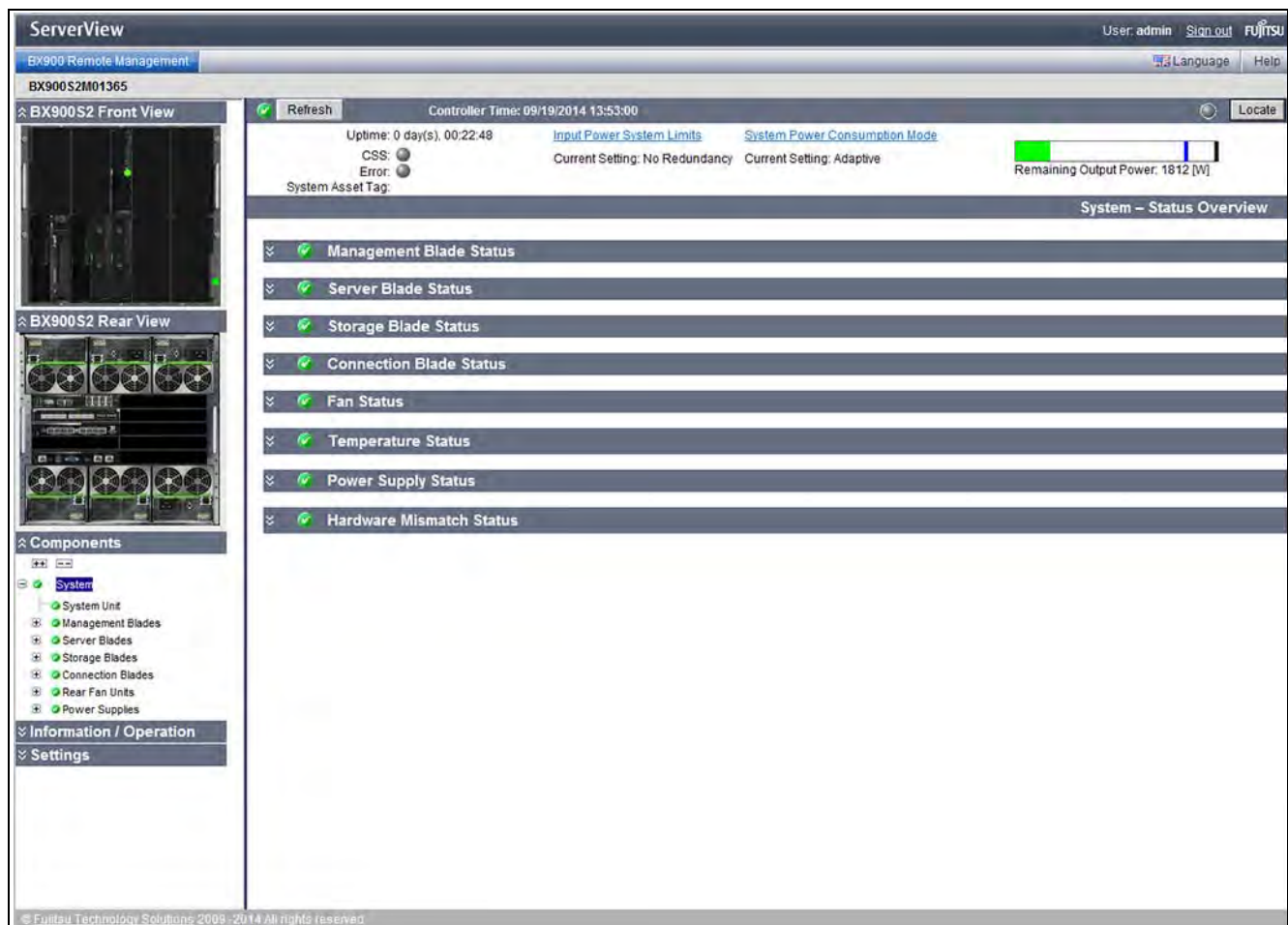


Figure 69: Check eDirectory login

7 Web User Interface Icons Overview

	Status	OK: All components are operating without error.
	Status	A device is not installed.
	Event severity	Informational.
	Status/Event severity	Warning or PDA Error. Severity: minor.
	Event severity	Major.
	Status/Event severity	Critical.
	CSS LED	An error of the type Warning or PDA Error has occurred in the system.
	CSS LED	When the amber icon is in the blinking state, it is not a warning or PDA Error but indicates a Critical Error.
	Error LED	An error of the type Warning or PDA Error has occurred in the system.
	Error LED	When the red icon is in the blinking state, it is not a warning or PDA Error but indicates a Critical Error.
	Location LED	Indicates that the MMB's ID LED is on.
	Power LED	System unit power state: switched on.
	LED off	No CSS, error or locate indication; system unit switched off.
	CSS: warning	One or more components which should be replaced by the customer are in a warning state.
	CSS: critical	One or more components which should be replaced by the customer are in a critical state.
	Toolbox symbol	Indicates a customer self service event log.
	Tools symbol	Indicates that a customer self service event log has one or more resolutions.
	MMB role	Master MMB.
	MMB role	Slave MMB.
	Door status	Open door in a floor-stand system.
	Door status	Closed door in a floor-stand system.
	MMB USB status	USB device connected to an MMB USB port (Advanced User Interface).
	MMB USB status	USB device connected to an MMB USB port (Standard User Interface).
	Storage association	Association between server blade and storage blade.
	Server blade indication	USB/DVD is assigned.

	Server blade indication	When the icon is in the blinking state it indicates that USB/DVD is assigned and in use.
	Server blade indication	USB/DVD is not assigned.
	Server blade indication	A console is active.
	Server blade indication	No console is active.
	Server blade indication	Button to switch the server blades on/off.
	Server blade indication	The server blade is in pre-processing mode, e.g. inventory or VIOM boot process
	Server blade indication	The server blade is in maintenance mode, e. g. during iRMC/BIOS flash process.
	Power bar	Powered off.
	Power bar	Powered on.
	Power bar	PSU is cordless/powering off.
	Consumption mode	Activated, activation in progress.
	Consumption mode	Not active.
	Help reference	Refers to more detailed information in the help text which is marked there with 

Abbreviations

AD

Active Directory

ACPI

Advanced Configuration Power Interface

AES

Advanced Encryption Standard

ARP

Address Resolution Protocol

ASCII

American Standard Code for Information Interchange

ASR

Automatic System Recovery

AuDi-MIP

Automatic Distribution of Management IP Addresses for PRIMERGY Blade Systems

BIOS

Basic Input Output System

BTU/h

British Thermal Unit per hour

CA

Certification Authority

CD-ROM

Compact Disk-Read Only Memory

CLI

Command Line Interface

CLP

Command Line Protocol

CMOS

Complementary Metal Oxide Semiconductor

CPU

Central Processor Unit

CSR

Certificate Signing Request

CSS

Customer Self Service

DC

Direct Current

DDR

Double Data Rate

DHCP

Dynamic Host Configuration Protocol

DIMM

Dual-in-Line Memory Module

DIP

Dual In-Line Package

DMTF

Distributed Management Task Force

DNS

Domain Name Server

DST

Daylight Saving Time

DVD

Digital Versatile Disk

EEPROM

Electrical Erasable Programmable Read Only Memory

EULA

End User License Agreement

EMP

Emergency Management Port

EPOW

Early Power Off Warning

FC

Fibre Channel

FRU

Field Replaceable Unit

GbE

Gigabit Ethernet

GUI

Graphical User Interface

GUID

Globally Unique Identifier

HDD

Hard Disk Drive

HTTP

Hypertext Transfer Protocol

HTTPS

Hypertext Transfer Protocol Secure

HW

Hardware

IBP	Intelligent Blade Panel
ICE	Import Convert Export
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IPMB	Intelligent Platform Management Bus
IPMI	Intelligent Platform Management Interface
iRMC	integrated Remote Management Controller
ITS	Invitation to Send
KVM	Keyboard, Video, Mouse
L2	Layer 2 (Data Link Layer)
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDIF	Lightweight Directory Interchange Format
LED	Light Emitting Diode
LSB	Local Service Display for Blades
MB	Megabyte
MD5	Message Digest 5
MMB	Management Blade

MUX	Multiplexer
N/A	Not Applicable
NDS	Novell Directory Services
NIC	Network Interface Card
NMI	Non-Maskable Interrupt
NTP	Network Time Protocol
OCP	OverCurrent Protection
OEM	Original Equipment Manufacturer
OOB	Out Of Band
OVP	OverVoltage Protection
OS	Operating System
PCI	Peripheral Component Interconnect
PDA	Prefailure Detection Analysis
PIN	Personal Identity Number
PROM	Programmable Read Only Memory
PSU	Power Supply Unit
PXE	Preboot eXecution Environment
PWOK	Power OK
RBS	Role-Based Services
RC4	Rivest Cipher 4

REMCS

Remote Customer Support System

RMS

Reliant Monitor Services

ROM

Read Only Memory

RPM

Rotations / Revolutions Per Minute

RSA

Rivest, Shamir, Adleman

RTC

Real Time Clock

RX

Receiver Cross

SDR

Sensor Data Records

SDRAM

Synchronous Dynamic Random Access Memory

SEL

System Event Log

SHA

Secure Hash Algorithm

SM CLP

Server Management Command Line Protocol

SMASH

Systems Management Architecture for Server Hardware

SNMP

Simple Network Management Protocol

SSH

Secure Shell

SSL

Secure Socket Layer

TCP/IP

Transmission Control Protocol/Internet Protocol

TFTP

Trivial File Transfer Protocol

TLS

Transport Layer Security

TPM

Trusted Platform Module

TX	Transmitter Cross
UART	Universal Asynchronous Receiver Transmitter
UI	User Interface
UID	Unit Identification Light
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USM	User-based Security Model
UVP	UnderVoltage Protection
VAC	Volts Alternating Current
VACM	View-based Access Control Model
VIOM	Virtual I/O Manager
VLAN	Virtual Local Area Network
WWN	World Wide Name
XML	Extensible Markup Language

Related Publications

PRIMERGY manuals are available in PDF format on the ServerView Suite DVD 2.

The PDF files for the manuals can also be downloaded free of charge from the Internet. The overview page showing the online documentation available in the Internet can be found via the URL: <http://manuals.ts.fujitsu.com> (for the EMEA market) and <http://primeserver.fujitsu.com/primergy/manual.html> for the Japanese market).



You will find further useful information in the documentation for your operating system.

- [1] **PRIMERGY BX900 S1 Blade Server**
Operating Manual
- [2] **PRIMERGY BX900 Blade Servers**
Manuals for various connection blade
- [3] **ServerView Deployment Manager**
User Manual
- [4] **BIOS Setup**
in Operating Manuals for server blades
- [5] **ServerView Installation Manager**
User Guide
- [6] **ServerView Operations Manager**
User Guide
- [7] **PRIMERGY ServerView Suite**
ServerView Virtual-IO Manager
User Guide

